KOMPUTERSWIAT.PL

Komputer Świat SPECIAL

MEMBER OF Computer GROUP

1/2019 (13) GRUDZIEŃ 2018 – LUTY 2019 CENA 14,90 ZŁ W TYM 8% VAT

NA DVD
50 NAJLEPSZYCH PROGRAMÓW
do anonimowości i zabezpieczania danych

3 PEŁNE WERSJE
o wartości 470 zł w KŚ+

Windows 200 SUPERTRIKÓW

- usprawnij i dobrze zabezpiecz **swoje Wi-Fi**
- **zaszyfruj i ukryj** twoje poufne pliki
- bądź **anonimowy** w internecie

WSZYSTKO O VPN
BEZPIECZNIE I ANONIMOWO W INTERNECIE – poradnik

SUPERPAKIET NA DVD
10 najlepszych darmowych VPN-ów

ETYCZNY HAKING
POZNAJ METODY HAKERÓW
Włam się do swojego Wi-Fi, by sprawdzić zabezpieczenia

PRAKTYCZNE I CIEKAWE TRIKI DO EXCELA
i innych programów **Microsoft Office**

WINDOWS Z PENDRIVE'A
Poznaj darmowy, ratunkowy system MediCat z **Windows PE**

KROK PO KROKU

JAK ZWIĘKSZYĆ ZASIĘG WI-FI
- przegląd najlepszych **rozwiązań** i **narzędzi**

W NUMERZE RÓWNIEŻ

ODZYSKIWANIE PLIKÓW w praktyce: poradnik i najlepsze darmowe narzędzia

DARMOWY MS OFFICE W SMARTFONIE z Androidem

NAS: ZRÓB WŁASNĄ CHMURĘ na swoje prywatne pliki – poradnik

ISSN 2083-3814 NR INDEKSU 276 065

9 772083 381901 01

Read + Think = Speak English

3

NAJPOPULARNIEJSZE POZIOMY NAUCZANIA

KONTEKSTOWE WIDEO UZUPEŁNIAJĄCE TREŚĆ ARTYKUŁÓW

+

NAGRANIA Z PROFESJONALNYM BRYTYJSKIM LEKTOREM

CZYTASZ ZE ZROZUMIENIEM, POPRAWIASZ WYMOWĘ, SPRAWDZASZ POSTĘPY — WSZYSTKO W

1,5h

EFEKTYWNA NAUKA W ŚWIETNEJ CENIE

POSZERZANIE HORYZONTÓW JĘZYKOWYCH JESZCZE NIGDY NIE BYŁO TAK PROSTE I PRZYJEMNE

PIERWSZY OPINIOTWÓRCZY MIESIĘCZNIK DO NAUKI ANGIELSKIEGO

W SPRZEDAŻY

W KIOSKACH I SALONACH PRASOWYCH

SPIS TREŚCI

NA START

Pełna wersja w KŚ+: Ashampoo WinOptimizer 2018 4
Pełna wersja w KŚ+: Ashampoo UnInstaller 6 5
Pełna wersja w KŚ+: Wise Registry Cleaner PRO 5

TRIKI DO SYSTEMU

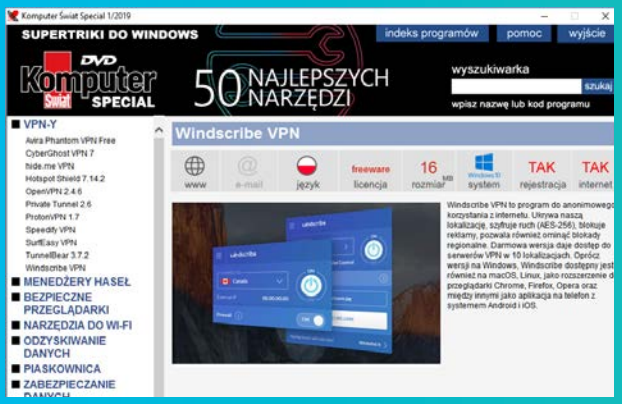
Co nowego w jesiennym uaktualnieniu October 2018 Update 6
Zarządzanie aktualizacjami Windows 10 12
Triki do Windows 10 14
Ustawienia, triki i zabezpieczenia do Windows 10 16
Kompleksowe rozwiązanie do kontroli rodzicielskiej 18
10 wskazówek do Menedżera zadań 20
Win PE – Windows na pendrivie 22
Połączenie smartfona z Androidem lub iOS do PC z Windows 10 24

TRIKI DO PROGRAMÓW

8 wskazówek do Office Online 26
10 wskazówek do OneDrive'a 28
8 wskazówek do Outlooka i Outlook.com 30
14 wskazówek do Excela 32
7 wskazówek do Worda 36
8 wskazówek do PowerPointa 38
10 wskazówek do Zdjęcia Windows 10 40
Ciekawe rozszerzenia do MS Edge 42
Bezpieczne przeglądarki 44
Zabezpieczanie danych – szyfrowanie 46
Odzyskiwanie danych w praktyce 50
Odzyskiwanie danych – najlepsze programy 52
Sandboksowanie programów 54
Menedżery haseł 56
Aplikacje Microsoftu na smartfonach z Androidem 58
Anonimowe systemy operacyjne 60

TRIKI DO INTERNETU

Bezpieczne korzystanie z otwartego Wi-Fi 62
Ustaw swój ruter 64



NASZA PŁYTA

Na płycie znajdziemy narzędzia opisane we wskazówkach: **superpakiet 101 najlepszych VPN-ów**, menedżery haseł, bezpieczne przeglądarki, narzędzia do usprawniania Wi-Fi, programy do odzyskiwania danych, bezpieczną piaskownicę dla programów, narzędzia do szyfrowania, aplikację do kontroli rodzicielskiej, Windows ADK do stworzenia pendrive'a ze specjalną wersją Windows PE i anonimowe systemy operacyjne. Dodatkowo na płycie jest też **duży dział z narzędziami do instalacji i reinstalacji Windows**.

Zabezpieczamy sieć Wi-Fi 68
Ataki w sieci domowej 72
Zbadaj swoją sieć bezprzewodową 76
8 sposobów, jak poprawić działanie Wi-Fi w domu 80
VPN – anonimowe i bezpieczne przeglądanie internetu 84
8 najciekawszych programów do VPN-ów 88
Konfiguracja dysku sieciowego NAS 90
Dwuetapowa weryfikacja 94
Specjalne skrzynki e-mail – tymczasowe i szyfrowane 96

NA KONIEC

9 prostych sposobów na zapewnienie sobie prywatności w internecie 98

CO TO JEST DVD-KOD

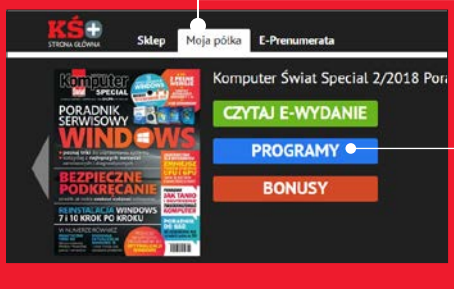
Aby szybko odnaleźć wybrany program, podaną za słowem **DVD-KOD** liczbę należy wpisać w wyszukiwarkę w menu płyty i zatwierdzić, wciskając klawisz enter

JAK POBRAĆ E-WYDANIE, ISO Z OBRAZEM PŁYTY I DODATKOWE PROGRAMY

E-wydanie magazynu, obraz ISO płyty dodanej do tego numeru i pełne wersje oraz dodatkowe programy znajdziemy w serwisie KŚ+ (**www.ksplus.pl**).

1 Otwieramy w przeglądarce stronę o adresie **www.ksplus.pl**. Logujemy się, klikając na **Logowanie** (używamy konta z serwisu Komputer swiat.pl). Jeżeli nie mamy konta, klikamy na **Załóż konto**, aby się zarejestrować.

2 Po zalogowaniu się rejestrujemy unikalny kod nadrukowany na płycie dołączonej do tego wydania magazynu. Wystarczy kliknąć na **Zarejestruj kod** i przepisać go.



3 Mamy już dostęp do e-wydania – aby je zobaczyć, wystarczy wejść na zakładkę **Moja półka** i kliknąć na okładkę cyfrowej wersji magazynu.

4 Aby przejrzeć e-wydanie lub pobrać PDF, klikamy na **Czytaj e-wydanie**. PDF pobierzemy, klikając na . A jeśli chcemy pobrać obraz ISO płyty lub pełne wersje czy dodatkowe aplikacje, klikamy na **Programy**.

NA START
PEŁNE WERSJE

Skutecznie odinstalowuje programy

ASHAMPOO WINOPTIMIZER 2018

PEŁNA WERSJA O WARTOŚCI 129 ZŁ

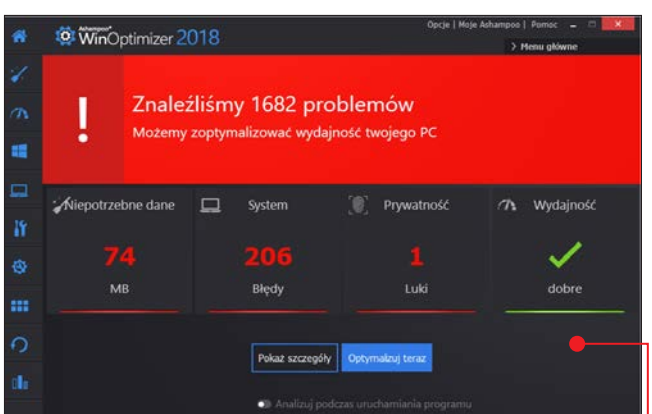
producent Ashampoo
internet www.ashampoo.com
system Windows 7, 8/8.1, 10
język polski
ograniczenia licencja na rok
rejestracja wymagana

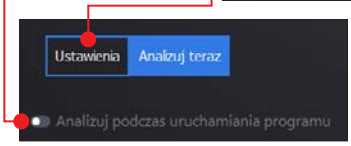
Do pobrania z www.ksplus.pl

Program do optymalizacji i przyspieszania Windows: czyści, przyspiesza i zabezpiecza system. Eliminuje też problemy powstające podczas normalnego używania komputera. Na szczególną uwagę zasługuje funkcja **optymalizacji jednym kliknięciem**, która szybko i sprawnie usuwa zbędne pliki zajmujące miejsce na dysku, naprawia skróty i czyści historię przeglądania wraz z plikami cookies. WinOptimizer pozwala tak zmienić ustawienia Windows, by **ograniczyć do niezbędnego minimum telemetrię**, czyli zbieranie danych o działaniu systemu i przesyłanie ich do producenta.

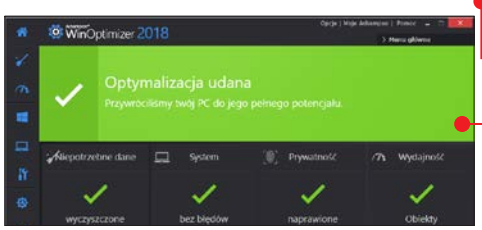
SKANOWANIE

1 By zacząć proces skanowania, w głównym oknie klikamy na **Analizuj teraz**. Klikając na ●, możemy zmienić domyślne ustawienia skanowania. Możemy także włączyć automatyczną analizę podczas uruchamiania programu ●.





2 Skanowanie może zająć chwilę. Na koniec program wyświetla podsumowanie ●. Aby zobaczyć szczegóły ●, klikamy na **Pokaż szczegóły**.



3 Klikamy na **optymalizuj teraz**, by naprawić wszystkie błędy naraz. Oto efekt ●.

FUNKCJE PROGRAMU

WinOptimizer to rozbudowany program. Z jego modułami możemy zapoznać się, klikając na ikony z lewej strony okna. Są to kolejno: **Sprzątanie systemu** A, **Poprawa wydajności** B, **Ustawienia Windows** C, **Analiza systemu** D, **Narzędzia plikowe** E, **Funkcje podstawowe** F (ustawienia programu), **Ostatnie kopie** G (przywracanie systemu do stanu sprzed zmian), **Statystyki** H. Aby zobaczyć wszystkie funkcje programu w jednym oknie, klikamy na I.

A – tu znajdziemy **One Click Optimizer** – optymalizację systemu jednym kliknięciem, narzędzia do zwalniania miejsca na dysku, sprzątania rejestru i czyszczenia śladów w przeglądarkach Internet Explorer, Firefox, Chrome, Safari, Opera, Edge.

B – narzędzia do zarządzania usługami Windows, optymalizacji uruchamiania systemu, optymalizacji połączenia internetowego, zarządzania działającymi procesami i odinstalowywania programów.

C – łatwy dostęp do ustawień Windows (między innymi opcje logowania czy wiadomość powitalna), **AntySpy**, czyli konfiguracja systemowych ustawień prywatności, **Menedżer menu kontekstowego**.

D – między innymi informacje o systemie, **DiskSpace Explorer**, czyli narzędzie do analizy zajętości miejsca na dysku, test wydajności systemu, **HDD Benchmark** – test wydajności dysków twardych, **HDD Inspector** – raporty o stanie dysków.

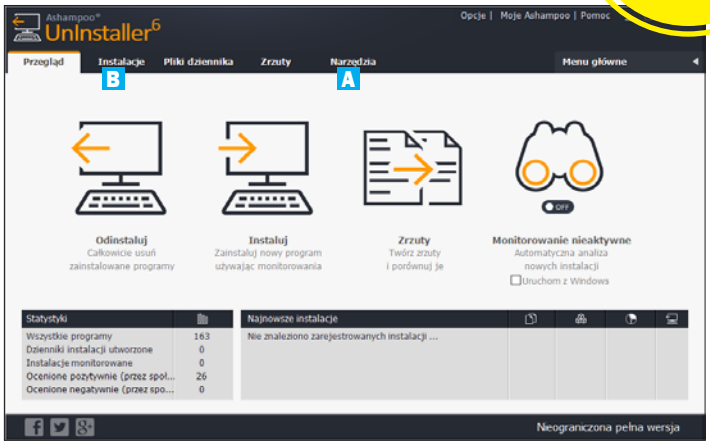
E – **File Wiper** – bezpowrotne wymazywanie danych, **File Manipulator** – szyfrowanie, zabezpieczanie hasłem oraz dzielenie i łączenie plików.

Skutecznie odinstalowuje programy

ASHAMPOO UNINSTALLER 6

PEŁNA WERSJA O WARTOŚCI **199** ZŁ

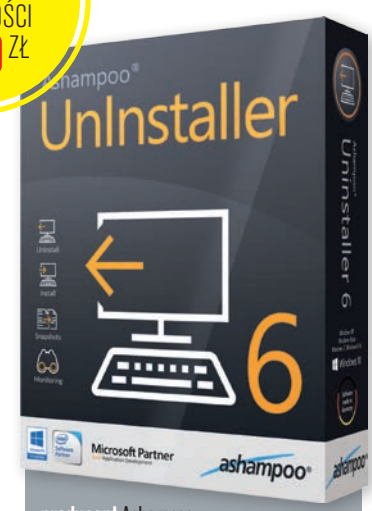
Narzędzie do dokładnego odinstalowywania programów i kontrolowania instalacji. Całkowicie usuwa niechciane aplikacje. Ma funkcję monitorowania instalacji wykrywającą niechciane dodatki w instalatorach pobranych z internetu i pozwalającą na ich łatwe usunięcie. Program rejestruje instalowane pliki i zapisywane wartości w rejestrze, dzięki czemu może je potem usunąć bez pozostawiania śladów. Działa znacznie skuteczniej niż rozwiązanie wbudowane w Windows. Przeprowadza głębokie czyszczenie pozostałości po aplikacjach. Umożliwia odinstalowywanie kilku aplikacji naraz. Zawiera narzędzia do sprzątania systemu (**Narzędzia** A) – czyści rejestr i dysk, defragmentuje dyski. Pozwala na przeprowadzenie gruntownych porządków.



Odinstalowujemy

1 Aby odinstalować program, klikamy u góry okna na **Instalacje** B. Przeglądamy listę programów. Możemy skorzystać z filtra, na przykład by wyszukać uszkodzone lub niepoprawnie odinstalowane aplikacje.

2 Zaznaczamy programy. Klikamy na **Odinstaluj**. Uruchamia się kreator odinstalowywania – cały proces przebiega automatycznie.



producent Ashampoo
internet www.ashampoo.com/pl
system Windows 7, 8, 10
język polski
ograniczenia brak
rejestracja wymagana

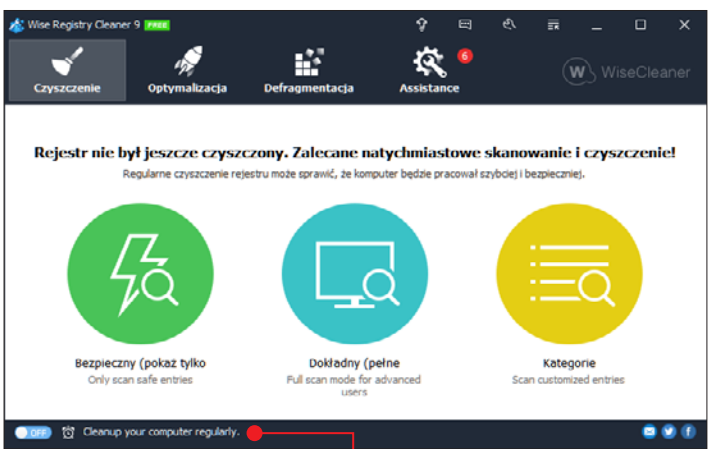
Do pobrania z www.ksplus.pl

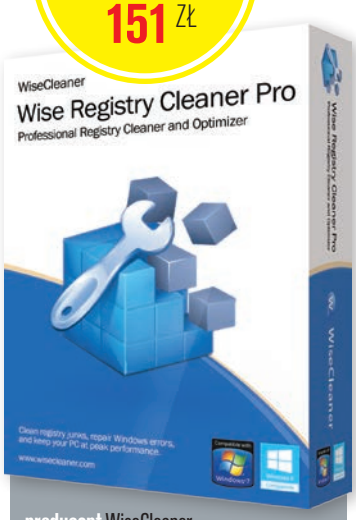
Oczyszcza i optymalizuje rejestr

WISE REGISTRY CLEANER PRO

PEŁNA WERSJA O WARTOŚCI **151** ZŁ

Wise Registry Cleaner skanuje rejestr systemu, znajduje błędy oraz zbędne elementy w rejestrze, a następnie usuwa je lub przeprowadza defragmentację. Co ważne, program automatycznie zapisuje kopie zapasowe rejestru, zanim rozpocznie porządki. Można również ręcznie w dowolnym momencie utworzyć pełną kopię zapasową rejestru lub punkt przywracania systemu. Pozwala to w razie problemów przywrócić komputer do stanu sprzed zmian.
Ważną funkcją wersji PRO jest **Multi-user Cleaning Pro**. Funkcja ta została opracowana z myślą o komputerach używanych przez więcej niż jedną osobę. Dzięki niej użytkownik z uprawnieniami administratora może skanować i czyścić rejestr na kontach wszystkich użytkowników jednocześnie, bez konieczności logowania się na każde z nich. Wygodna jest też możliwość planowania automatycznego czyszczenia rejestru zgodnie z dziennym, tygodniowym lub miesięcznym harmonogramem. Ciekawostka to możliwość utworzenia na pulpicie skrótu pozwalającego przeprowadzać czyszczenie rejestru jednym kliknięciem.
Wise Registry Cleaner może również zoptymalizować ustawienia Windows, aby poprawić szybkość zarówno systemu, jak i internetu.





producent WiseCleaner
internet www.wisecleaner.com
system Windows XP, Vista, 7, 8/8.1, 10
język polski
ograniczenia brak aktualizacji
rejestracja wymagana

Do pobrania z www.ksplus.pl

TRIKI DO SYSTEMU
PAŹDZIERNIKOWA AKTUALIZACJA WINDOWS 10

CO NOWEGO

W październiku Microsoft udostępnił publicznie ***szóstą dużą aktualizację Windows 10****. To October 2018 Update, które rozwijano pod nazwą kodową Redstone 5.* ***Nie obyło się jednak bez problemów*** *i Microsoft musiał wycofać aktualizację oraz poprawić system. Mimo to pojawiło się* ***kilka ciekawych nowości*** *oraz udoskonalenia istniejących funkcji. Zobaczmy, co nowego wprowadzono w Windows 10 October 2018 Update*

Windows 10 October 2018 Update to bardzo duże uaktualnienie do najpopularniejszego systemu operacyjnego na świecie. To już szósta aktualizacja tego typu, którą rozwijano pod nazwą kodową Redstone 5. Niestety, nie obyło się bez problemów, o czym możemy przeczytać w ramce poniżej. Nowa wersja okienek wprowadza sporo nowości. Pojawiła się nowa aplikacja **Twój telefon**, która stanowi pomost pomiędzy komputerem z Windows i smartfonem z Androidem. W ten sposób można między innymi wysyłać SMS-y czy przeglądać zdjęcia przechowywane w pamięci telefonu z Androidem. Wprowadzono też wiele innych nowości w powłoce systemu, sekcji **Ustawienia** oraz przeglądarce **Microsoft Edge**. Przyjrzyjmy się z bliska najciekawszym nowym funkcjom. **dd**

PROBLEMY

Październikowa aktualizacja dla Windows 10 okazała się bardzo problematyczna. Największe problemy sprawiły dwa błędy. Pierwszy spowodował utratę danych użytkowników przechowywanych na dysku. To właśnie z tego powodu po kilku dniach od udostępnienia Windows 10 October 2018 Update Microsoft zdecydował się wycofać uaktualnienie. Kolejny błąd dotyczył rozpakowywania archiwów. W specyficznych scenariuszach mogło dojść do nadpisania plików. W momencie gdy czytacie ten artykuł, październikowe uaktualnienie prawdopodobnie znowu jest dostępne, zapewne już bez wymienionych błędów.

SPRAWDZAMY WERSJĘ ZAINSTALOWANEGO WINDOWS 10

Istnieje prawdopodobieństwo, że na naszym komputerze jest już zainstalowany Windows 10 October 2018 Update. Microsoft dystrybuował to uaktualnienie przez kilka pierwszych dni października poprzez Windows Update. Jeśli chcemy sprawdzić wersję naszego systemu, to musimy wykonać następujące czynności.

1 Naciskamy klawisze ⊞ + R i wpisujemy polecenie **winver**, które należy zatwierdzić klawiszem enter.

2 Po chwili uruchomi się okno o nazwie **Windows – informacje**. To właśnie tutaj należy odszukać numer wersji zainstalowanego oprogramowania. Można to zrobić w sekcji **Wersja**.

3 Jeśli w sekcji **Wersja** pojawia się liczba **1809**, to oznacza, że na komputerze jest już zainstalowany Windows 10 October 2018 Update. Jeżeli numer jest niższy, to jest to jedna z poprzednich wersji okienek.

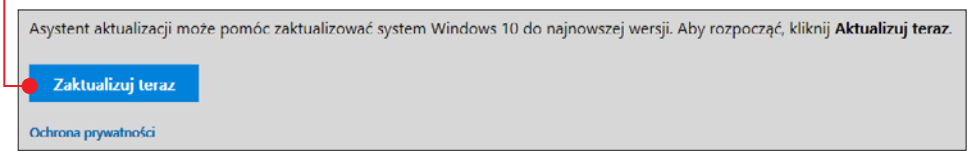
WYKONUJEMY RĘCZNĄ INSTALACJĘ AKTUALIZACJI

Nic nie stoi jednak na przeszkodzie, aby zainstalować Windows 10 October 2018 Update ręcznie. Microsoft udostępnia duże uaktualnienia etapami. To oznacza, że w Windows Update może ono pojawić się nawet po wielu tygodniach od premiery. Zobaczmy więc, jak wykonać instalację z użyciem narzędzia **Asystent aktualizacji**.

1 W przeglądarce internetowej wpisujemy adres **https://www.microsoft.com/pl-pl/software-download/windows10**, skąd pobierzemy narzędzie.

2 Klikamy na przycisk **Zaktualizuj teraz**, który rozpocznie pobieranie Asystenta aktualizacji.

3 Uruchamiamy pobrane narzędzie i postępujemy zgodnie ze wskazówkami wyświetlanymi na ekranie. Instalator uaktualnienia sprawdzi nasz sprzęt pod kątem zgodności i następnie zrestartuje komputer kilka razy, (jest to normalne zachowanie w trakcie instalowania dużych aktualizacji do systemu Windows 10).



W JESIENNYM UAKTUALNIENIU OCTOBER 2018 UPDATE

TWÓJ TELEFON

Dawid Długosz
autor

Twój telefon to jedna z najważniejszych nowości, które wprowadza Windows 10 October 2018 Update. To przebudowana aplikacja, która stanowi pomost pomiędzy komputerem i smartfonem. Na najwięcej możliwości mogą obecnie liczyć użytkownicy smartfonów z Androidem. Opcje dostępne dla iPhone'ów zostaną dodane z czasem. Zobaczmy, jakie możliwości oferuje nowa aplikacja.

Aktualizacje Windows 10 ostatnio nieco straciły na jakości i stabilności. Microsoft co pół roku chce wprowadzić możliwie jak najwięcej nowych funkcji, co cieszy. Niestety, nie idzie z tym w parze odpowiedni poziom oprogramowania. Najlepszym dowodem jest wycofanie niedługo po premierze October 2018 Update. Zresztą wiosenne uaktualnienie April 2018 Update również zawierało błędy. Co prawda nie doszło do wstrzymania dostępności systemu, ale Microsoft i tak miał do rozwiązania niemało problemów. Może lepszym wyjściem byłoby udostępnianie dużych aktualizacji nie co pół roku, ale co dwanaście miesięcy. Wtedy gigant z Redmond miałby więcej czasu na sprawdzenie działania całego systemu i być może obyłoby się bez problemów, z którymi spotykamy się teraz.

ŁĄCZYMY TELEFON Z KOMPUTEREM Z WINDOWS 10

Android*

Chcąc synchronizować zawartość smartfona z Androidem na komputerze z Windows 10 October 2018 Update, najpierw trzeba połączyć urządzenie z PC. Jest to dosyć prosta czynność. W tym celu należy wykonać poniższe kroki.

1 Uruchamiamy aplikację **Twój telefon** i klikamy na przycisk **Rozpocznij**.

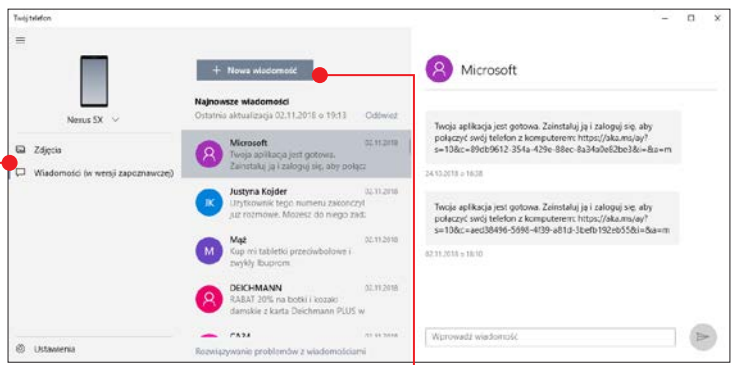
2 W nowym oknie podajemy numer telefonu, na który Microsoft wyśle wiadomość SMS.

3 Dotykamy odnośnika znajdującego się w SMS-ie od Microsoftu. W ten sposób zostaniemy przeniesieni do Sklepu Play, skąd trzeba pobrać aplikację o nazwie **Pomocnik aplikacji Twój telefon**. Jeśli wiadomość SMS nie dochodzi, można udać się pod adres **https://play.google.com/store/apps/details?id=com.microsoft.appmanager**, skąd pobierzemy aplikację.

4 Uruchamiamy zainstalowanego pomocnika i logujemy się do niego z użyciem tego samego konta Microsoftu, którego używamy na komputerze z Windows 10. Potem musimy już tylko wskazać nasz komputer i zezwolić aplikacji na dostęp do SMS-ów i zdjęć. Możemy rozpocząć pracę z aplikacją Twój telefon.

PRZEGLĄDAMY I WYSYŁAMY SMS-Y

Przydatna funkcja aplikacji Twój telefon to możliwość przeglądania wiadomości SMS ze smartfona. Chcąc to zrobić, klikamy na sekcję **Wiadomości (w wersji zapoznawczej)** – po chwili wyświetli się lista ostatnich wiadomości tekstowych. Oczywiście, możemy przeglądać cały wątek. Wystarczy tylko na niego kliknąć. Najciekawszą opcją jest jednak możliwość wysyłania SMS-ów z poziomu komputera z Windows 10. Klikamy na przycisk **Nowa wiadomość** i następnie wpisujemy jej treść oraz numer osoby, do której SMS ma zostać wysłany.



* Kod QR szybko przenosi na stronę, skąd można pobrać aplikację. Skanujemy go smartfonem za pomocą dowolnej aplikacji QR pobranej z Google Play

JAK PRZYWRÓCIĆ SYSTEM DO STANU SPRZED AKTUALIZACJI, JEŚLI COŚ PÓJDZIE NIE TAK, MOŻNA PRZECZYTAĆ W **POPRZEDNIM WYDANIU KOMPUTER ŚWIAT SPECIAL 2/2018** DOSTĘPNYM W KS+ **WWW.KSPLUS.PL**

TWÓJ TELEFON NA RAZIE NIE DLA IPHONE'ÓW

Możliwości aplikacji Twój telefon, które poznaliśmy na przykładzie smartfona z Androidem, nie mają jednak zastosowania w przypadku iPhone'ów. Co prawda telefon z iOS można sparować z aplikacją, ale na wiele się to nie zda. Nie przejrzymy zdjęć. Nie będziemy mogli także przeglądać wiadomości. Microsoft twierdzi, że pracuje nad zapewnieniem podobnych funkcji użytkownikom iPhone'ów, ale na ich wprowadzenie trochę sobie jeszcze poczekamy. Na razie możliwe jest tylko przesyłanie stron wyświetlanych w przeglądarce Edge na iPhonie bezpośrednio na komputer z Windows 10.

PRZEGLĄDAMY ZDJĘCIA Z TELEFONU

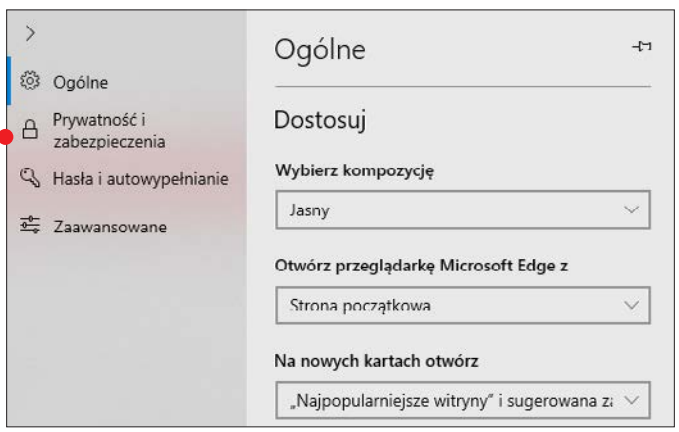
Twój telefon pozwala na wygodne przeglądanie zdjęć, które znajdują się w rolce aparatu smartfona z Androidem. Niestety, taka możliwość dotyczy tylko ostatnich 25 fotografii z telefonu. Więcej zobaczyć się nie da. Fotki wyświetlane są w galerii. Oczywiście, fotografie można powiększać. Dwukrotne kliknięcie na którąkolwiek z nich powoduje uruchomienie aplikacji Zdjęcia z Windows 10. W tej aplikacji można edytować fotkę lub też szybko udostępnić ją znajomym.

LAWINA NOWOŚCI W MICROSOFT EDGE

Microsoft Edge to wbudowana w Windows 10 przeglądarka internetowa – następca Internet Explorera. Edge wraz z aktualizacją Windows 10 October 2018 Update doczekał się wielu nowych funkcji. Poznajmy najciekawsze z nich.

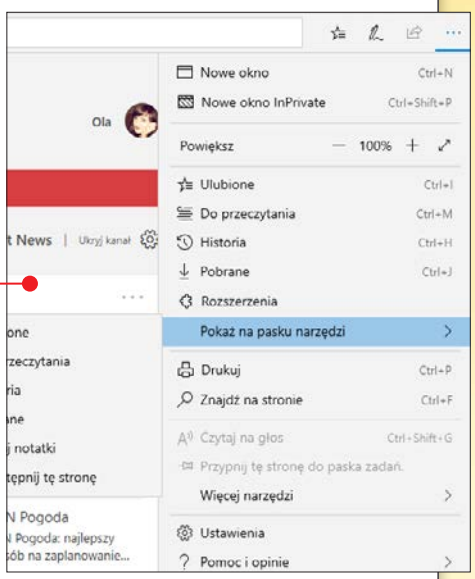
PRZEBUDOWANE USTAWIENIA

Microsoft zdecydował się przebudować ustawienia przeglądarki Edge. W końcu poszczególne opcje podzielono na osobne sekcje tematyczne, co pozwala łatwiej odnaleźć się w gąszczu wielu różnych ustawień. Sekcje te to **Ogólne**, **Prywatność i zabezpieczenia**, **Hasła i autowypełnianie** i **Zaawansowane**.



ODŚWIEŻONE MENU

Microsoft postanowił także odświeżyć menu w przeglądarce Edge. Wraz z Windows 10 October 2018 Update zobaczymy, że po naciśnięciu przycisku z trzema kropkami po prawej stronie pojawi się przebudowane menu. Uproszczono je, aby dostęp do poszczególnych opcji był łatwiejszy. Tutaj znajduje się też opcja **Pokaż na pasku narzędzi**. W tym miejscu można szybko dodać lub usunąć elementy, które będą wyświetlane po prawej stronie adresu.



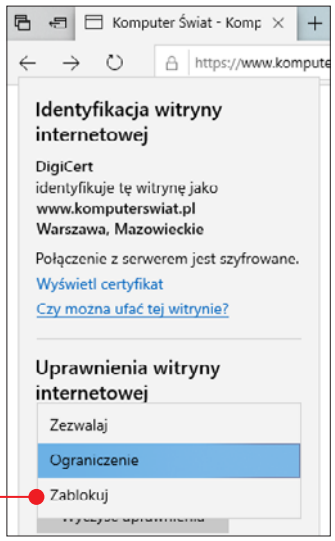
AUTOODTWARZANIE MULTIMEDIÓW POD KONTROLĄ

Microsoft Edge w końcu pozwoli zapanować nad autoplayerami umieszczanymi na stronach internetowych. To od nas będzie teraz zależeć, które ze stron będą mogły automatycznie odtwarzać multimedia. Zobaczmy, jak to można robić.

1 Uruchamiamy stronę internetową, dla której chcemy wprowadzić zmiany, i klikamy na ikonę kłódki po lewej stronie paska adresu.

2 Przechodzimy do sekcji **Ustawienia witryny internetowej** i rozwijamy listę **Autoodtwarzanie multimediów**.

3 Domyślnie włączona jest opcja **Zezwalaj**, ale możemy wybrać inną – **Ograniczenie** lub **Zablokuj**. Ta ostatnia powoduje całkowitą blokadę autoodtwarzania. Wyjaśnienie opcji **Ograniczenie** – patrz ramka obok.

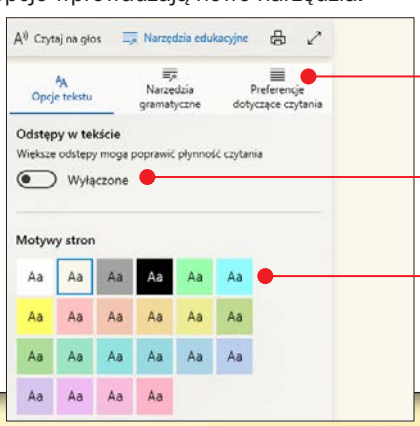


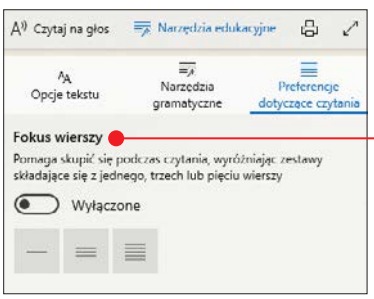
OPCJA OGRANICZENIE

Jeśli zdecydujemy się na wybór opcji **Ograniczenie** na liście Autoodtwarzanie multimediów, sprawimy, że filmy nie będą się same włączać, gdy wideo jest z wyciszonym dźwiękiem. Jednak kliknięcie na dowolne miejsce tej strony sprawi, że autoodtwarzanie uruchomi się ponownie.

PREFERENCJE DOTYCZĄCE CZYTANIA I OPCJE TEKSTU

Windows 10 October 2018 Update w sekcji **Narzędzia edukacyjne** wprowadza dwa nowe panele. To **Opcje tekstu** oraz **Preferencje dotyczące czytania**. Trzeci, czyli **Narzędzia gramatyczne**, został uaktualniony. Zobaczmy, jakie opcje wprowadzają nowe narzędzia.





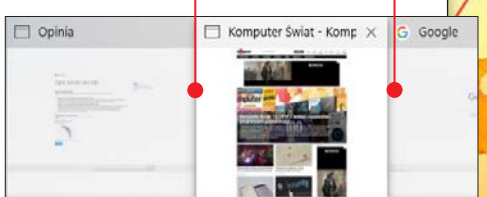
W sekcji **Opcje tekstu** możemy włączyć większe odstępy w tekście, co może ułatwić czytanie. Jest też możliwość zmiany motywu strony. Do wyboru mamy ponad 20 opcji. **Preferencje dotyczące czytania** zawierają opcję o nazwie **Fokus wierszy**. Jej włączenie ma pomagać skupić się na czytanym tekście. Polega to na wyróżnianiu zestawów składających się z jednego, trzech lub pięciu wierszy.

BARDZIEJ BEZPIECZNA PRZEGLĄDARKA

Microsoft Edge po aktualizacji do Windows 10 October 2018 Update w końcu wspiera **Web Authentication**. Dzięki temu można logować się na stronach bez użycia haseł. W zamian otrzymujemy nowe możliwości, jak czytnik linii papilarnych, mechanizm odpowiadający za rozpoznawanie twarzy czy PIN. Jest też wsparcie dla rozwiązań opartych na technologii FIDO, która umożliwia szybkie uwierzytelnianie na podstawie danych biometrycznych.

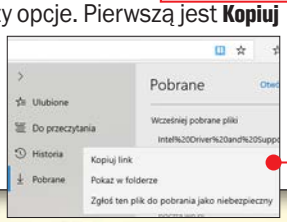
NOWE ELEMENTY FLUENT DESIGN

Microsoft Edge już w poprzednich aktualizacjach dla Windows 10 dostał wsparcie dla elementów nowego języka projektowania, czyli **Fluent Design**. Wraz z październikową aktualizacją pojawiają się kolejne, niewielkie modyfikacje, które bazują na tym rozwiązaniu. Przykładowym jest lepsze wyeksponowanie na górnym pasku tej karty, która jest aktywna. To efekt głębi, który znajduje się na kartach po prawej i lewej stronie.



NOWE OPCJE W SEKCJI POBRANYCH PLIKÓW

Jeśli w Microsoft Edge przejdziemy do sekcji **Pobrane**, to znajdziemy tu ostatnio ściągnięte z internetu pliki. Klikamy na jeden z nich prawym przyciskiem myszy. Zobaczymy nowe menu kontekstowe, w którym umieszczono trzy opcje. Pierwszą jest **Kopiuj link**. Następnie mamy **Pokaż w folderze**. Ostatnią jest możliwość zgłoszenia witryny jako niebezpiecznej. Wtedy zostaniemy przeniesieni na specjalną stronę, gdzie będziemy mogli dokonać zgłoszenia.



WIĘCEJ ZMIAN I NOWOŚCI

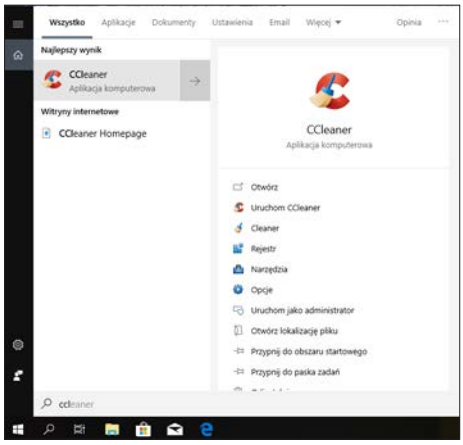
NOWOŚĆ W SEKCJI BLUETOOTH

Sekcja ustawień dla Bluetooth z Windows 10 October 2018 Update otrzymała ważną nowość – informacje o stanie naładowania baterii poszczególnych urządzeń, które mają akumulatory i komunikują się z komputerem drogą bezprzewodową. Chcąc to zobaczyć, musimy udać się do sekcji **Ustawienia**, **Urządzenia i Bluetooth**. Tutaj wyświetlane są wskaźniki procentowe.

Niestety, dotyczy to tylko urządzeń Microsoftu, jak rysik Surface Pen czy Dial. W przypadku pozostałych sprzętów taka obsługa pewnie pojawi się później.

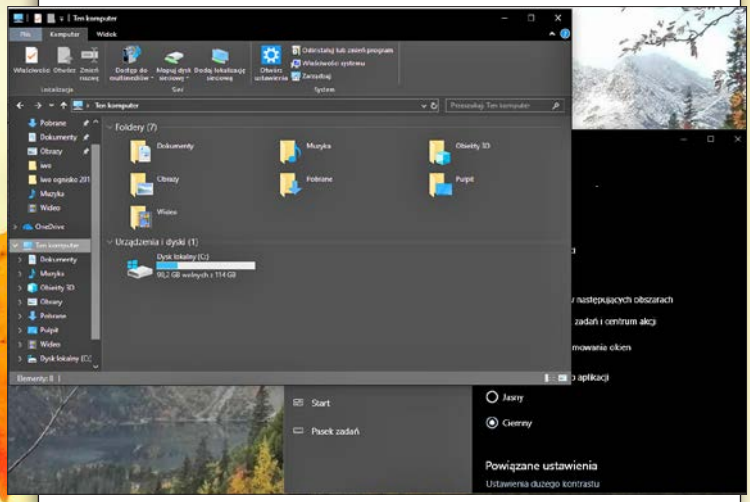
WIĘCEJ MOŻLIWOŚCI W MENU START

Menu Start z Windows 10 October 2018 Update też doczekało się udoskonaleń. Najważniejszą nowością jest więcej akcji dla poszczególnych aplikacji, które wyszukujemy poprzez wbudowaną wyszukiwarkę. Dla przykładu, po wyszukaniu CCleanera mamy znacznie więcej możliwości, niż tylko uruchomienie aplikacji. Możemy od razu włączyć jeden z wybranych składników programu, w tym Cleaner, Rejestr czy Narzędzia. To miłe usprawnienie, ale trzeba mieć na uwadze, że tego typu opcje wyświetlane są tylko przy wybranych programach.



TRYB CIEMNY W EKSPLORATORZE PLIKÓW

Microsoft długo przymierzał się do zapewnienia obsługi dla trybu ciemnego w Eksploratorze plików. W końcu udało się tego dokonać wraz z październikową aktualizacją Windows 10. To oznacza, że jeśli wybierzemy w ustawieniach kolorów opcję **Ciemny** dla **Wybierz domyślny tryb aplikacji**, to Eksplorator plików również dopasuje się do naszego wyboru i nie będzie jasnym oknem, jak to było dotychczas.



WIELE NOWYCH EMOJI

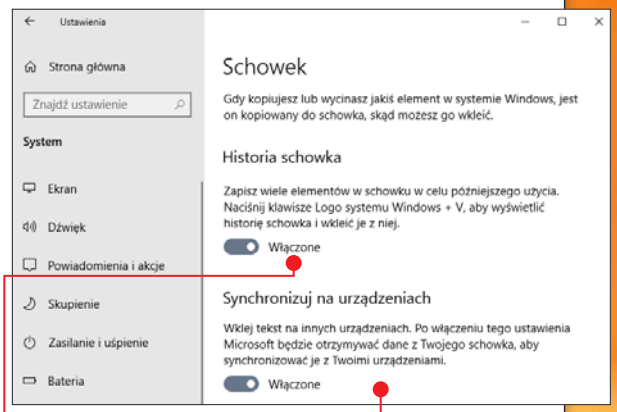
Windows 10 October 2018 Update wprowadza także wiele nowych emoji. To emotki, które pojawiły się w aktualizacji Unicode 11 z czerwca 2018 roku. Aktualizacja wprowadza ponad 70 nowych obrazków, a część istniejących zmodyfikowano. Pojawił się kangur, ząb, deskorolka, pluszowy miś, papuga, rolka papieru toaletowego i wiele więcej. Panel z emoji można wywołać, wciskając klawisze ⊞ + .

PROGRAM NIEJAWNYCH TESTÓW WINDOWS NIE DLA WSZYSTKICH

Program niejawnych testów systemu Windows skierowany jest do bardziej zaawansowanych użytkowników. To oznacza, że możemy do niego dołączyć, jeśli godzimy się na ewentualne błędy i nieoczekiwane problemy, które mogą powodować dyskomfort w trakcie użytkowania komputera. Poglądowych wersji Windows 10 najlepiej też nie instalować na głównym komputerze, który użytkowany jest do pracy, ale na innej maszynie, gdzie stabilna praca oprogramowania nie będzie miała dla nas większego znaczenia. Można też zdecydować się na instalację na maszynie wirtualnej.

HISTORIA SCHOWKA MOŻE BYĆ SYNCHRONIZOWANA

Schowek to funkcja Windows, którą znamy i której używamy od lat. Przez ostatni czas doczekała się wielu udoskonaleń. Nie ogranicza się do prostej czynności, czyli kopiowania i wklejania. Schowek pozwala obecnie na synchronizację w chmurze – dzięki temu można kopiować i wklejać elementy pomiędzy różnymi urządzeniami. Wraz z Windows 10 October 2018 Update ta możliwość zostaje rozszerzona o historię schowka. Teraz, kiedy wciśniemy na klawiaturze klawisze ⊞ + V, zostanie wyświetlona historia, którą można przeglądać, a następnie w jej oknie zdecydować się na wybór elementu do wklejenia. Chcąc włączyć historię schowka, należy wykonać następujące czynności.



1 Udajemy się do ustawień schowka, które znajdziemy w sekcji **Ustawienia** i **System**.

2 Następnie trzeba włączyć opcję **Historia schowka**. Zawartość będzie synchronizowana, jeśli jest aktywna opcja **Synchronizuj na urządzeniach** znajdująca się niżej.

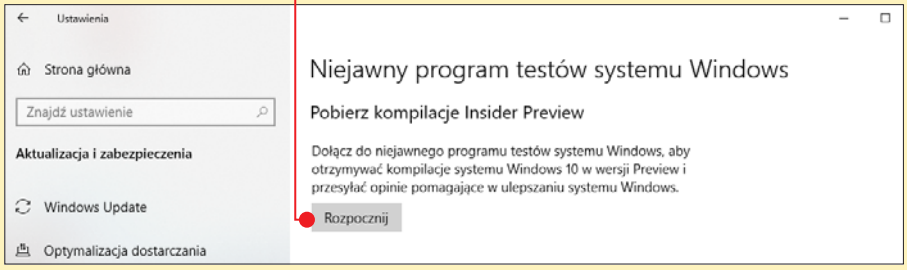
NOWOŚCI DLA ZAAWANSOWANYCH UŻYTKOWNIKÓW

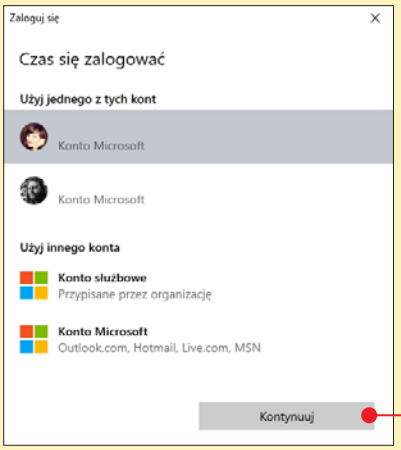
Jeśli to, co znalazło się w Windows 10 October 2018 Update, to ciągle dla nas za mało, możemy dołączyć do niejawnego programu testów systemu Windows. Wtedy zostaniemy beta testerami i uzyskamy dostęp do kolejnej, już siódmej dużej aktualizacji dla nowych okienek. **Windows 10 19H1**, bo pod takim kryptonimem powstaje kolejne uaktualnienie, jest już testowane z członkami programu Insider. Przystępując do programu, już teraz można wypróbować nowe funkcje przed innymi – finalna wersja Windows 10 19H1 ma być gotowa dopiero wiosną 2019 roku.
Zobaczmy, jak dołączyć do programu pilotażowego.

1 Przechodzimy do sekcji **Ustawienia**, a następnie **Aktualizacja i zabezpieczenia**.

2 Udajemy się do sekcji **Niejawny program testów systemu Windows**.

3 W nowym oknie trzeba kliknąć na przycisk **Rozpocznij**.





4 Wybieramy konto, z którym chcemy dołączyć do programu, i klikamy na przycisk **Kontynuuj**.

5 Potem będziemy musieli wybrać konkretny kanał programu, na przykład **szybki pierścień aktualizacji**.

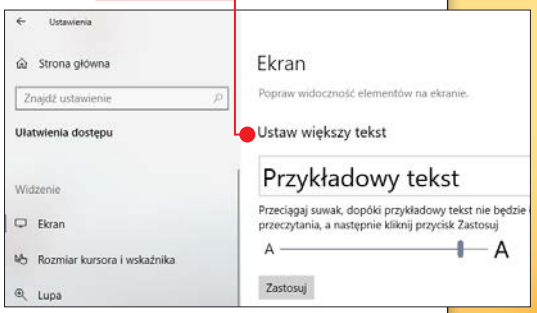
6 Na końcu pozostanie zainstalować nową wersję oprogramowania, która zostanie pobrana poprzez usługę Windows Update.

WYGODNE POWIĘKSZANIE TEKSTU

Październikowa aktualizacja dla Windows 10 to także nowe narzędzie do powiększania tekstu wyświetlanego na ekranie komputera. W ten sposób można w wygodny sposób zwiększyć rozmiar czcionki w całym systemie operacyjnym. Chcąc tego dokonać, należy wykonać następujące czynności.

1 Udajemy się do sekcji **Ustawienia**, **Ułatwienia dostępu** i **Ekran**.

2 Tutaj znajdziemy suwak **Ustaw większy tekst**, który łapiemy kursorem myszy



i przesuwamy w prawą stronę aż do momentu uzyskania odpowiedniego efektu. Wielkość tekstu będzie generowana na żywo w okienku znajdującym się nad suwakiem. Rozmiar można zwiększyć maksymalnie do 225 procent.

Fot. Jakub Gojda/123rf.com

TRIKI DO SYSTEMU
JAK AKTUALIZOWAĆ WINDOWS

DZANIE

*Nieaktualizowany system to zagrożenie, ale **brak kontroli nad aktualizacjami może być frustrujący**. Oto jak sobie z tym radzić w Windows 10*

Nieaktualizowany system operacyjny to zagrożenie. Niezałatana luka to potencjalne wejście do systemu dla agresora. Znane hakerom luki w niezaktualizowanym systemie mogą być skutecznie wykorzystane nawet w sytuacji, gdy mamy najnowszy antywirus.

Co do zasady, automatyczne aktualizacje systemu operacyjnego powinny być zawsze włączone. To dzięki nim system ma łatane luki zabezpieczeń i otrzymuje co jakiś czas nowe funkcje. W wersji Windows 10 Home Microsoft wymusił takie działanie systemu, że funkcja automatycznych aktualizacji jest domyślnie aktywna, a one same instalują się możliwie najszybciej po ich publikacji przez producenta.

Dla wielu osób takie ustawienie systemu jest wygodne. Nie trzeba pamiętać o aktualizacjach i zawsze mamy najnowszą wersję systemu operacyjnego z załatanymi lukami zabezpieczeń.

Niektórych użytkowników funkcja automatycznych aktualizacji jednak irytuje i chcieliby mieć większą kontrolę nad tym, co, kiedy i w jaki sposób jest instalowane. Dotyczy to także firm, które mogą mieć własną strategię aktualizacji komputerów stanowiących elementy firmowej infrastruktury.

Zobaczmy, jak zarządzać aktualizacjami w najpopularniejszej edycji Windows 10 Home oraz jakie dodatkowe możliwości w zakresie zarządzania aktualizacjami oferuje Windows 10 Pro. **as**

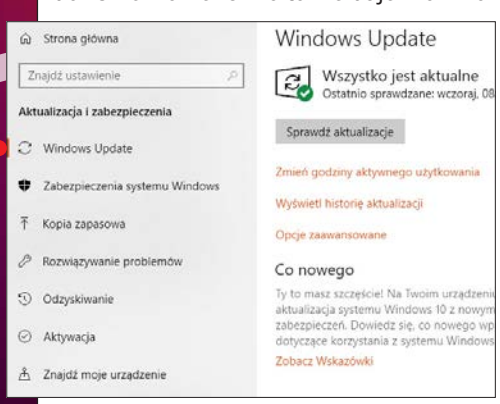
ZARZĄDZANIE AKTUALIZACJAMI W WINDOWS 10 HOME

Microsoft znacząco ograniczył możliwość konfigurowania ustawień dotyczących aktualizacji systemowych w tej wersji Windows. Oto co możemy zrobić

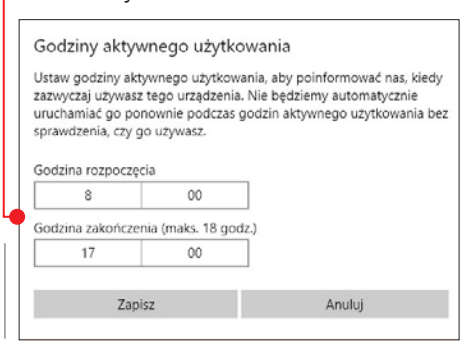
USTAWIANIE GODZIN, GDY AKTUALIZACJA NIE BĘDZIE PRZESZKADZAĆ

1 Dostęp do ustawień aktualizacji w Windows 10 uzyskamy, wywołując okno **Ustawienia** (najszybciej – skrótem klawiaturowym ⊞+I), a następnie wybierając ikonę **Aktualizacja i zabezpieczenia**.

2 W kolejnym oknie domyślnie powinna być zaznaczona sekcja **Windows Update**. Po prawej stronie wyświetlany jest stan aktualizacji systemu oraz opcje dostępne w Windows 10 Home. Okno to nie daje możliwości wyłączenia automatycznych aktualizacji, ale możliwe jest ustawienie systemu w taki sposób, by komputer nie uruchamiał się ponownie z powodu aktualizacji w czasie, gdy pracujemy. W tym celu klikamy na odnośnik **Zmień godziny aktywnego użytkowania**.

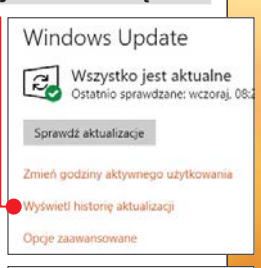


3 Wyświetlona zostanie ramka, w której możemy zdefiniować godziny pracy na komputerze, podczas których Windows nie powinien uruchamiać się ponownie w wyniku pobrania i instalacji aktualizacji. Tym samym eliminujemy ryzyko, że w czasie pracy czy grania komputer zostanie zrestartowany.

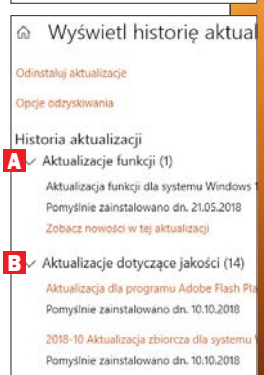


CO ZMIENIA DANA AKTUALIZACJA

1 W bardzo łatwy sposób możemy dotrzeć do informacji na temat zmian wprowadzanych w systemie przez konkretny pakiet aktualizacyjny. W oknie **Windows Update** klikamy na odnośnik **Wyświetl historię aktualizacji**.



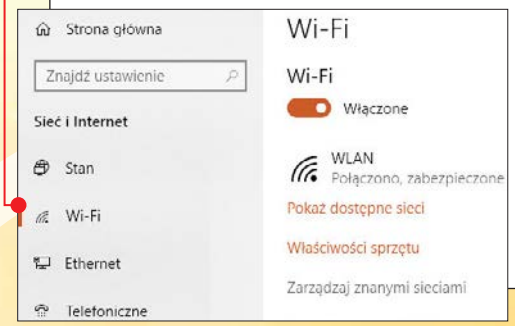
2 W kolejnym oknie zobaczymy listę zainstalowanych w systemie aktualizacji pogrupowanych w odrębne kategorie (takie jak **Aktualizacje funkcji** A czy **Aktualizacje jakości** B). Po rozwinięciu danej kategorii wpis dotyczący każdej aktualizacji jest jednocześnie linkiem, na który kliknięcie spowoduje otwarcie w przeglądarce strony z dokładnym opisem danego pakietu aktualizacyjnego.



AKTUA AMI W WINDOWS 10

BLOKOWANIE AKTUALIZACJI W WINDOWS 10 HOME

W Windows 10 Home nie da się całkowicie wyłączyć aktualizacji, ale można zablokować ich pobieranie (a tym samym instalację), stosując pewien trik. W domyślnych ustawieniach aktualizacje automatyczne nie są pobierane, gdy komputer korzysta z połączenia taryfowego – czyli łącza internetowego, które jest płatne. Chodzi o to, by proces aktualizacji nie obciążał dodatkowo kieszeni użytkownika. Trik polega na tym, by aktualne połączenie (na przykład z domową siecią Wi-Fi) ustawić jako taryfowe.

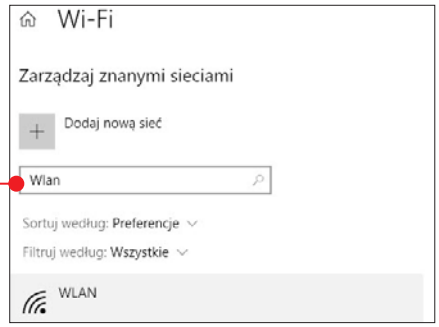


1 Wywołujemy okno **Ustawienia systemu Windows** (skrótem ⊞+I), a następnie klikamy na **Sieć i Internet**.

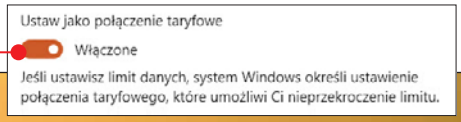
2 W kolejnym oknie zobaczymy stan sieci, z którą komputer jest w danej chwili połączony. W menu po lewej stronie klikamy na pozycję **Wi-Fi**. Potem po prawej stronie okna wybieramy **Zarządzaj znanymi sieciami**.

3 Pokaże się lista wszystkich sieci bezprzewodowych, z jakimi komputer kiedykolwiek się łączył. Ograniczamy ją wyłącznie do sieci, którą chcemy ustawić jako taryfową, wpisując jej nazwę (SSID) w pole w górnej części okna. Wybieramy nazwę odnalezionej sieci na liście i klikamy na **Właściwości**.

4 W kolejnym oknie, w sekcji **Połączenie taryfowe** ustawiamy przełącznik **Ustaw jako połączenie taryfowe** w pozycji **Włączone**. Od tej



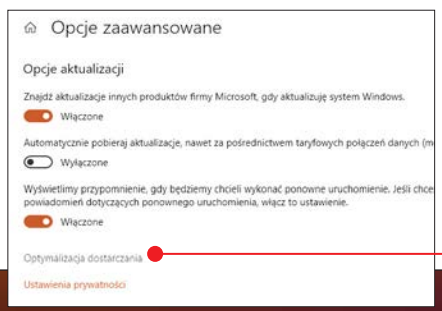
pory Windows nie będzie pobierać aktualizacji, gdy komputer będzie połączony z siecią określoną jako taryfowa. **Uwaga!** To rozwiązanie ma charakter tymczasowy, może wpływać na działanie również innych aplikacji sieciowych zainstalowanych w systemie i nie poleca się stosowania tej metody na dłuższą metę, gdyż system nieaktualizowany to system niebezpieczny.



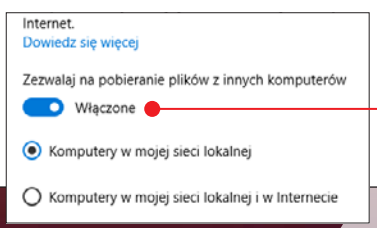
SZYBSZE POBIERANIE DZIĘKI OPTYMALIZACJI DOSTARCZANIA

1 Aktualizacje systemu Windows 10 to często znaczne ilości danych. Jeżeli mamy w domu kilka komputerów podłączonych do jednej sieci bezprzewodowej, możemy znacząco ograniczyć czas pobierania dużych aktualizacji na pozostałe komputery.

2 Otwieramy okno **Windows Update** i klikamy na **Opcje zaawansowane**.



3 W oknie **Opcje zaawansowane** klikamy na **Optymalizacja dostarczania**, a następnie w kolejnym oknie, w sekcji **Zezwalaj na pobieranie plików z innych komputerów** ustawiamy przełącznik **Zezwalaj na pobieranie plików z innych komputerów** w pozycji **Włączone**. Zaznaczamy opcję **Komputery w mojej sieci lokalnej**. Od tej pory wystarczy, że jeden z komputerów w domowej sieci pobierze duży pakiet aktualizacyjny z serwerów Microsoftu – pozostałe komputery przekopiują go już z maszyny, która pobrała go pierwsza.



AKTUALIZACJE W WINDOWS 10 PRO I ENTERPRISE

Użytkownicy i administratorzy profesjonalnych, korporacyjnych, a także edukacyjnych edycji Windows 10 mają znacznie większe możliwości zarządzania mechanizmem automatycznych aktualizacji systemu. W ich przypadku istnieje możliwość skorzystania z **Edytora zasad grup** (⊞+R i polecenie **gpedit.msc**). Za pomocą tego edytora można wpływać na działanie mechanizmu aktualizacji automatycznych poprzez szablon administracyjny o nazwie **Usługa Windows Update**. Znajdujące się w tym szablonie ustawienia pozwalają nie tylko na odłożenie aktualizacji systemu w czasie, ale też całkowite wyłączenie automatyki i przejście na ręczne instalowane pakietów aktualizacyjnych. Takie rozwiązanie ze względów bezpieczeństwa nie jest jednak zalecane.

Fot. Ievgenii Skryzhak/123rf.com

TRIKI
DO SYSTEMU
WINDOWS 10

TRIKI DO SYSTEMU WINDOWS 10

*Oto najciekawsze triki do systemu Windows 10, które pozwalają wykonywać **codzienne zadania szybciej i wygodniej**. Warto je poznać i zapamiętać!*

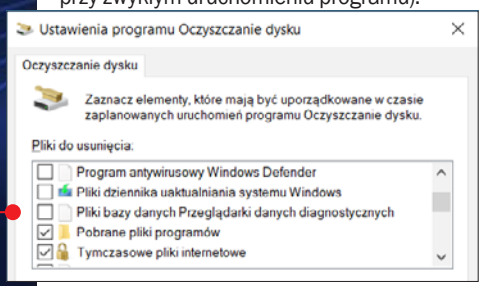
1 OCZYSZCZANIE DYSKU 1-CLICK

Narzędzie **Oczyszczanie dysku** w Windows zostało stworzone po to, by pomagać nam usuwać zbędne pliki i odzyskiwać miejsce na dysku. Ponieważ dostęp do niego i jego konfiguracja nie są zbyt wygodne, warto utworzyć skrót, który będzie automatycznie uruchamiał określone przez nas porządki.

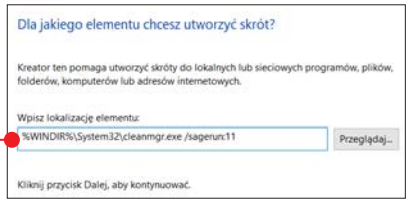
1 W pole wyszukiwania systemu wpisujemy **cmd**, a następnie klikamy prawym przyciskiem myszy na **Wiersz polecenia** i **Uruchom jako administrator**, a następnie na **Tak**.

2 Wpisujemy polecenie **%WINDIR%\System32\cleanmgr.exe /sageset:11** i wcis kamy enter.

3 Otworzy się okno ustawień narzędzia **Oczyszczanie dysku**. Zaznaczamy, które zbędne pliki mają być usuwane, i klikamy na **OK** (możliwości jest znacznie więcej niż przy zwykłym uruchomieniu programu).



4 Teraz tworzymy skrót na pulpicie, który będzie uruchamiał ustawione oczyszczanie: klikamy prawym przyciskiem myszy na pulpit, wybieramy **Nowy** i **Skrót**. W nowym oknie wpisujemy **%WINDIR%\System32\cleanmgr.exe /sagerun:11**, klikamy na **Dalej**, wpisujemy nazwę zadania i klikamy na **Zakończ**.

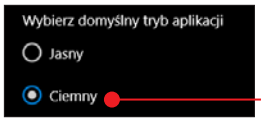


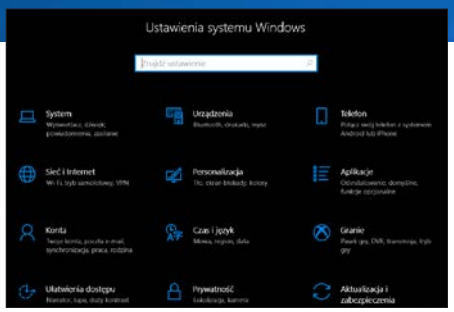
5 Po dwukrotnym kliknięciu na ikonę utworzonego skrótu rozpoczną się porządki.

2 CIEMNY TRYB DLA KAŻDEGO

W poprzednich wersjach Windows 10 uruchamianie ciemnego motywu dla całego systemu wiązało się z wykonywaniem skomplikowanych instrukcji. Ciemny tryb szczególnie docenić powinny osoby, które korzystają z komputera w godzinach nocnych, gdyż zbyt jasne okna systemu mogą powodować znacznie szybsze zmęczenie oczu. Po wielu systemowych aktualizacjach możemy uaktywnić ciemny tryb w łatwy sposób.

1 Klikamy na menu **Start**, **Ustawienia**, **Personalizacja**.





2 Następnie przechodzimy do kategorii **Kolory** i po lewej stronie zmieniamy **Domyślny tryb aplikacji** z **Jasny** na **Ciemny**. Od teraz wszystkie aplikacje systemu z designem MetroUI będą miały ciemny motyw.

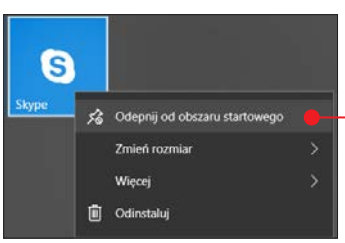
W najnowszej, październikowej aktualizacji Windows tryb ciemny można zastosować do Eksploratora Windows; więcej o jesiennej aktualizacji na stronie 6.

3 ZARZĄDZANIE KAFELKAMI

Menu Start w Windows 10 składa się z części stałej, której nie możemy modyfikować, listy programów oraz specjalnego obszaru, w którym można umieszczać aktywne kafelki. Część użytkowników chce pozbyć się wszystkich kafelków, część chce zarządzać nimi i tworzyć grupy programów. Oto jak robić jedno i drugie.

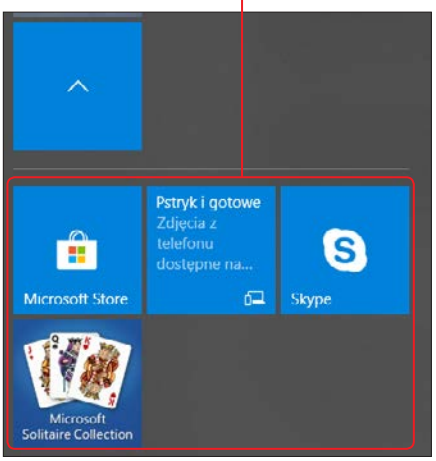
Usuwamy pole kafelków

Jeśli chcemy całkowicie pozbyć się widoku kafelków, wystarczy odpiąć wszystkie elementy kafelkowe, a pozostanie nam tylko menu programów. Klikamy na kolejne kafelki prawym przyciskiem myszy i wybieramy opcję **Odepnij od obszaru startowego**.



Tworzymy foldery na kafelki

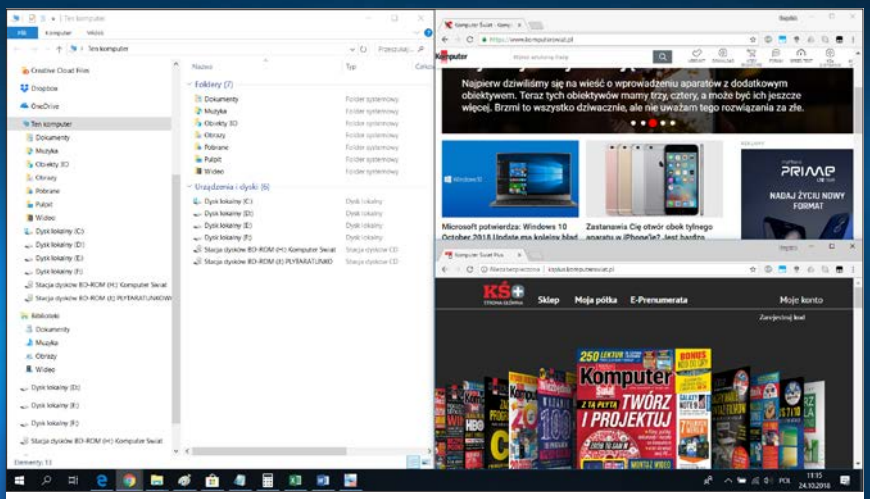
Po rozwinięciu menu Start wystarczy, że przeciągniemy jeden kafelek na drugi, a utworzony zostanie nowy folder. Otwieramy go, klikając na środku, pojawi się na nim symbol strzałki, a pod spodem pokazane zostaną wszystkie elementy umieszczone w danym folderze.



WS 10

4 POTRZĄSANIE I PORZĄDKOWANIE

Jest to funkcja, która była już dostępna we wcześniejszych wersjach systemu Windows, jednak niewielu użytkowników o niej wie. Korzystamy z niej wtedy, gdy na ekranie jest otwartych wiele różnych okien, a chcemy pracować tylko z jednym, a resztę zminimalizować. Zamiast pojedynczo minimalizować każde okno, możemy wykorzystać jeden prosty trik. Klikamy i przyciskamy lewy przycisk myszy na pasku tytułowym okna, które ma zostać na ekranie, i energicznie „potrząsamy" nim, wykonując ruchy w lewo i prawo. Wtedy wszystkie inne okna zostaną zminimalizowane, a program, którego pasek tytułowy trzymamy, pozostanie otwarty.

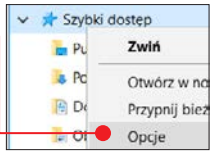


5 PRZYPINANIE OKIEN DO KRAWĘDZI EKRANU

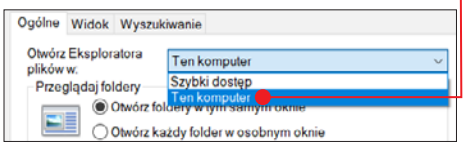
Jest to bardzo przydatny trik, który ułatwia podział obszaru roboczego na równe części. Wystarczy „przytrzymać" wybrane okno lewym przyciskiem myszy i przeciągnąć w kierunku wybranego przez nas rogu ekranu. Wskazane okno zostanie przeskalowane do 25 procent powierzchni ekranu i doklejone do wybranego rogu. Możemy również przeciąg nąć okno do wybranego przez nas boku ekranu, wtedy zajmie ono 50 procent ekranu. Przeciągając okno do górnej krawędzi, zmaksymalizujemy je.

6 DOMYŚLNE WYŚWIETLANIE OPCJI TEN KOMPUTER

Większość użytkowników, którzy przeszli z systemu Windows 7 na Windows 10, nie może pogodzić się z tym, że po uruchomieniu Eksploratora domyślnie otwiera się on w widoku **Szybki dostęp**, podczas gdy większość z nas woli korzystać ze starszego rozwiązania i rozpoczynać pracę z Eksploratorem w widoku **Ten komputer**.
Możemy bardzo szybko przywrócić tryb wyświetlania znany ze starszej wersji Windows. Musimy tylko uruchomić Eksplorator, kliknąć prawym przyciskiem myszy na **Szybki dostęp**, a w menu dialogowym kliknąć na **Opcje**.

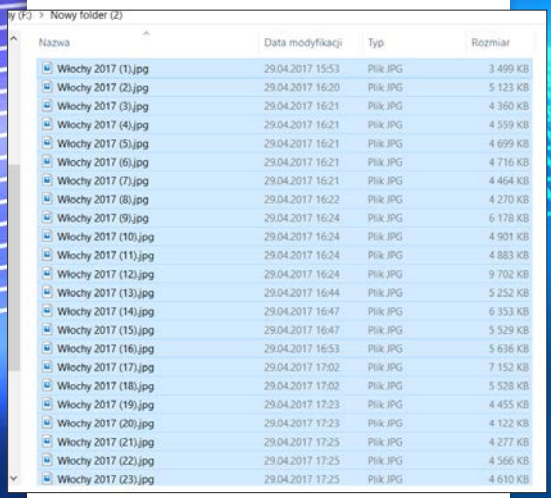


Teraz wystarczy, że w zakładce **Ogólne** ustawimy opcję **Otwórz Eksploratora plików w:**, **Ten komputer** i zapiszemy zmiany, klikając na **OK**. Po ponownym uruchomieniu eksploratora pojawi się od razu widok naszych dysków.



7 SZYBKIE MASOWE NADAWANIE NAZW PLIKOM

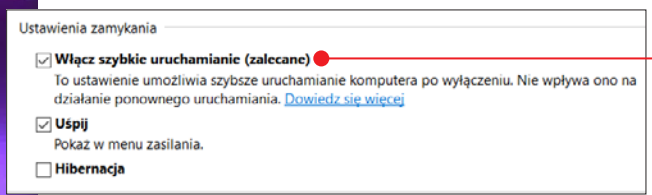
Ten trik pozwala nazwać wiele plików jednocześnie. Najczęściej może być nam potrzebny, gdy pracujemy z dużymi folderami z multimediami, a nazwy plików są bardzo różne i trudno jest się wśród nich zorientować.
Wystarczy, że w danym katalogu wciśniemy kombinację klawiszy Ctrl+A – w celu zaznaczenia wszystkich elementów, a następnie klawisz F2 i podamy nazwę pierwszego pliku. Reszta zostanie nazwana na wzór pierwszego elementu wraz z przypisaną odpowiednią liczbą porządkową. **kd**



Fot. Antishock/123rf.com

8 SZYBSZY START SYSTEMU WINDOWS

Dzięki temu trikowi nasz system może uruchamiać się szybciej. Klikamy prawym przyciskiem myszy na ikonę baterii na naszym komputerze i wybieramy **Opcje zasilania**. Następnie klikamy na **Wybierz działanie przycisków zasilania**. Teraz klikamy na **Zmień ustawienia, które są obecnie niedostępne**.



Poniżej zaznaczamy opcję **Włącz szybkie uruchamianie** i zapisujemy zmiany. Teraz nasz komputer powinien uruchamiać się znacznie szybciej. **kd**

TRIKI DO SYSTEMU *WINDOWS 10*

U NIA, TRI

Poznajmy ciekawe i przydatne, a mało znane ustawienia systemu Windows, które ***zwiększają wygodę, pomagają w pracy oraz poprawiają bezpieczeństwo***

TRYB GODMODE

CIEKAWOSTKA

Windows 10, podobnie jak starsze wersje systemu Microsoftu, również ma ukryty tryb GodMode (tryb boski). Czym on jest? GodMode jest nazwą specjalnego trybu, który daje dostęp do ukrytych w Windows funkcji. Rozwiązanie to prezentuje nam w inny sposób zawartość Panelu sterowania i okna Ustawienia, a także daje dostęp do funkcji, których tam nie ma, bo Microsoft celowo je ukrył.

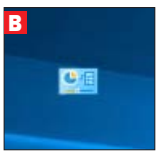
Jak aktywować GodMode w Windows 10

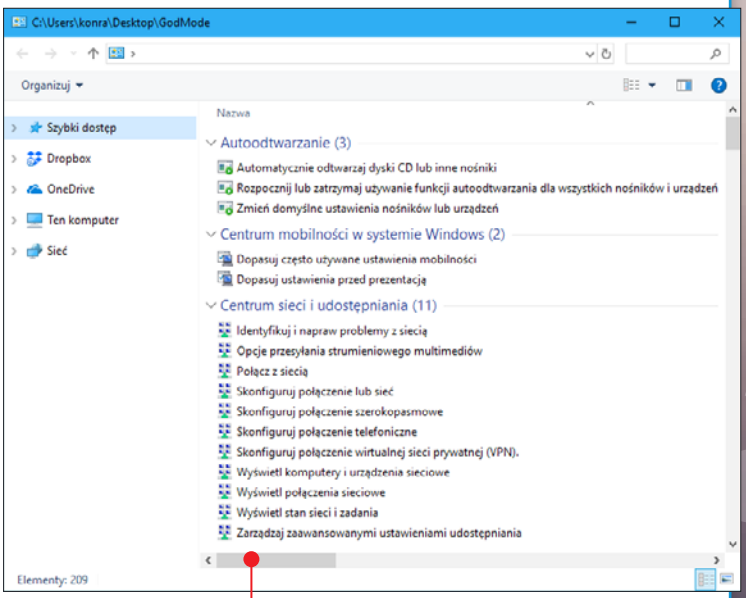
1 Aktywacja tego trybu możliwa jest jedynie z poziomu konta administratora. Najpierw upewniamy się zatem, że jesteśmy zalogowani na koncie z takimi właśnie uprawnieniami.

2 Jeśli tak – możemy zaczynać. Tworzymy nowy folder: klikamy prawym przyciskiem myszy na pulpit bądź w innej wybranej przez nas lokalizacji. Z rozwiniętego menu kontekstowego wybieramy **Nowy**, a następnie **Folder**.

3 Utworzony folder nazywamy: **GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}** A i zatwierdzamy klawiszem enter.

4 Folder zmienia swoją ikonę i ukrywa wpisany przez nas ciąg znaków B.





5 Gdy go otworzymy, uzyskamy dostęp do zaawansowanego panelu sterowania w trybie GodMode.

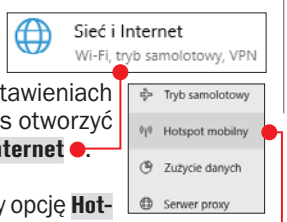
Uwaga! Pamiętajmy, aby nie eksperymentować z ustawieniami dostępnymi w GodMode, gdy nie mamy pewności co do przeznaczenia konkretnej funkcji.

Nie bez powodu twórcy systemu zdecydowali się na ukrycie pewnych opcji. Nieodpowiedzialne korzystanie z tego trybu może doprowadzić do problemów.

JAK UTWORZYĆ MOBILNY HOTSPOT

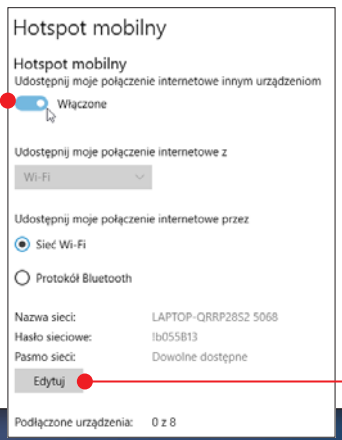
Co zrobić w sytuacji, kiedy ruter przestał działać, a potrzebujemy połączenia Wi-Fi w smartfonach lub tabletach? Wystarczy, że mamy laptop wyposażony w moduł Wi-Fi, do którego możemy podłączyć internet poprzez przewód – bezpośrednio z modemu. Laptop może posłużyć nam właśnie za ruter – wystarczy, że zrobimy z niego mobilny hotspot.

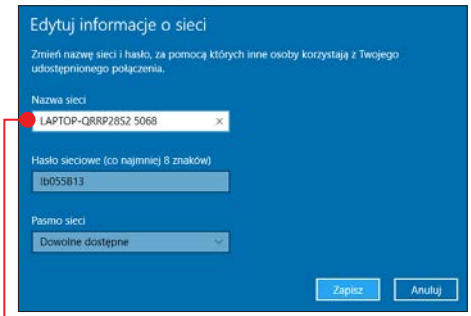
1 Aby utworzyć mobilny hotspot, należy w Ustawieniach systemu Windows otworzyć kategorię **Sieć i Internet**.



2 Tam wybieramy opcję **Hotspot mobilny** z menu bocznego.

3 Dalej w ustawieniach przełączamy na **Włączone** opcję **Udostępnij moje połączenie internetowe innym urządzeniom**.





4 Teraz pozostaje już tylko połączyć się z innego urządzenia z siecią Wi-Fi, której nazwa jest podana w polu, i uwierzytelnić się przez podane hasło.

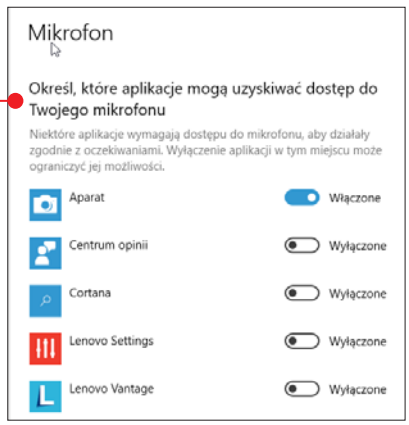
5 Jeśli będziemy chcieli zmienić nazwę sieci lub jej hasło – skorzystajmy z przycisku **Edytuj**, aby przejść do okna, w którym możliwe będzie wpisanie nowych danych sieci.

Fot. Orson/123rf.com, Vectorportal.com

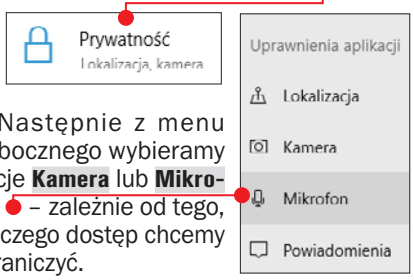
KI I ZAB ZENIA

JAK OGRANICZYĆ APLIKACJOM DOSTĘP DO KAMERY I MIKROFONU

Jeśli obawiamy się, że mikrofon i kamera w naszych urządzeniach mogą zostać wykorzystane do szpiegowania nas i naruszania naszej prywatności, możemy ograniczyć aplikacjom dostęp do nich.



1 W Ustawieniach systemu Windows należy wejść do kategorii **Prywatność**.



2 Następnie z menu bocznego wybieramy opcje **Kamera** lub **Mikrofon** – zależnie od tego, do czego dostęp chcemy ograniczyć.

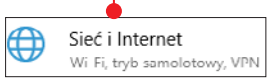
3 Widok opcji związanych z kamerą lub mikrofonem należy przewinąć nieco do dołu, aby znaleźć sekcję **Określ, które aplikacje mogą uzyskiwać dostęp do...**. Tam, przełączając przełączniki, możemy decydować, które aplikacje powinny mieć dostęp do mikrofonu (lub kamery).

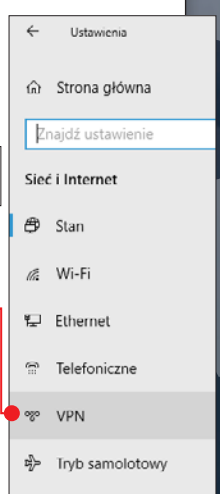
4 Pamiętajmy o tym, że niektóre z aplikacji bez udzielonego dostępu do mikrofonu czy kamery nie będą działać w pełni funkcjonalnie, dotyczy to na przykład komunikatorów takich jak Skype.

JAK OGRANICZYĆ TRANSFER DANYCH W SIECIACH TARYFOWYCH PRZY KORZYSTANIU Z VPN

Zdarza się, że korzystając z VPN-ów – czyli wirtualnych sieci prywatnych – pobieramy sporo danych. W domowych sieciach Wi-Fi nie zwracamy często uwagi na transfer. Inaczej jest, gdy korzystamy z połączeń taryfowych. Możemy jednak zablokować możliwość połączeń VPN w sieciach taryfowych.

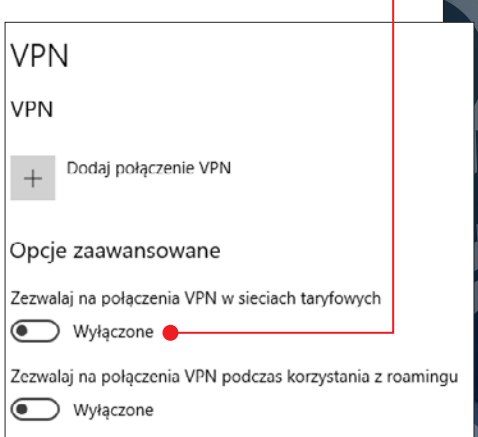
1 W **Ustawieniach systemu Windows** powinniśmy przejść do opcji **Sieć i Internet**.





2 Następnie z menu bocznego wybieramy pozycję **VPN**.

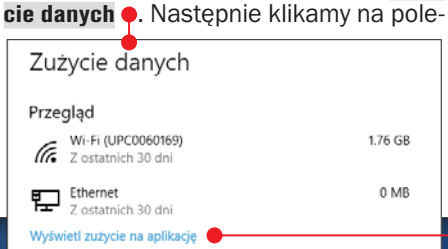
3 Teraz w sekcji **Opcje zaawansowane** powinniśmy przy pozycji **Zezwalaj na połączenia VPN w sieciach taryfowych** ustawić przełącznik na opcję **Wyłączone**.



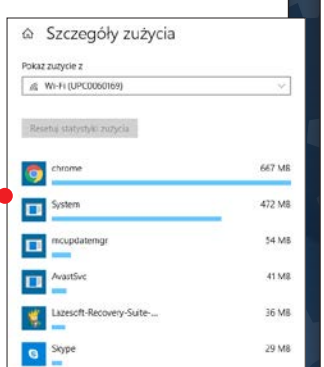
KTÓRE APLIKACJE ZUŻYWAJĄ NAJWIĘCEJ DANYCH INTERNETOWYCH

Sprawdzając, jak dużo danych z internetu pobraliśmy, możemy się nieraz bardzo zdziwić. Transfer może wydać nam się większy, niż przypuszczaliśmy. Często zużywają go aplikacje, które działają w tle, a my praktycznie z nich nie korzystamy. Jak identyfikować programy, które zużywają najwięcej transferu danych?

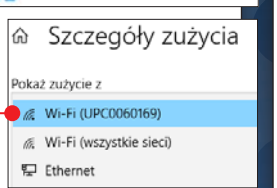
1 W Ustawieniach systemu Windows należy wejść do kategorii **Sieć i Internet**, gdzie z menu bocznego wybieramy pozycję **Zużycie danych**. Następnie klikamy na polecenie **Wyświetl zużycie na aplikację**.



2 Wyświetlone zostanie zestawienie, w którym widzimy, ile danych zostało zużytych przez każdy z programów.



3 Zestawienie to, możemy zmodyfikować, wybierając z jakiej sieci mają być wyświetlone dane.



KONTROLA RODZICI

Jeśli chcemy mieć kontrolę nad tym, ***jak nasze dziecko korzysta z urządzeń mobilnych, z zainstalowanych na nich aplikacji i z internetu****, wypróbujmy Rodzinę Microsoft lub narzędzie Kaspersky Safe Kids w darmowej wersji. Poznajmy te dwa rozwiązania*

RODZINA MICROSOFT

Aby korzystać z funkcji Rodzina Microsoft, trzeba mieć konto Microsoft. To bezpłatna usługa mająca zwiększać bezpieczeństwo dzieci korzystających z komputerów z **Windows 10**, konsoli **Xbox One** i **urządzeń z Androidem** z zainstalowaną aplikacją **Microsoft Launcher** (patrz też strona 58). Ustawienia, takie jak raportowanie aktywności, limity czasu korzystania z komputera, udostępnianie informacji o lokalizacji i ograniczenia dotyczące zawartości przeglądanych stron, są dostępne na stronie **account.microsoft.com/family**, gdzie można także śledzić wydatki dzieci i dodawać pieniądze do ich kont Microsoft. Aby móc korzystać z możliwości kontroli rodzicielskiej oferowanych przez system indywidualnych kont Microsoft, trzeba utworzyć wirtualną rodzinę kont i zaprosić do niej poszczególnych użytkowników. **kj**

JAK UTWORZYĆ GRUPĘ RODZINNĄ I DODAWAĆ DO NIEJ OSOBY

1 Aby utworzyć grupę rodzinną, powinniśmy udać się na stronę **https://account.microsoft.com/family**. Klikamy na **Utwórz grupę rodzinną**, po czym logujemy się na nasze (rodzica) konto Microsoft.

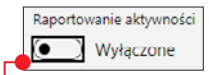
2 Zostajemy przeniesieni do okna dodawania nowego członka do rodziny. Możemy wpisać adres e-mail lub numer telefonu dziecka, jeśli ma ono konto Microsoft. Jeżeli go nie ma, klikamy na **Utwórz je dla niego** i tworzymy konto.

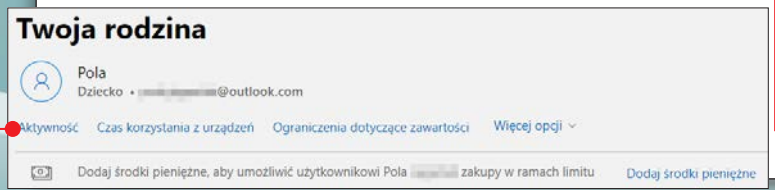
3 Jeżeli stworzyliśmy nowe konto, zostanie ono automatycznie dodane do rodziny. Jeśli dodając członka rodziny, użyliśmy istniejącego konta, na adres e-mail dziecka zostanie wysłana wiadomość z prośbą o akceptację dodania go do rodziny. Aby korzystać z konta dziecka, trzeba potwierdzić swoją tożsamość rodzica. Wymaga to podania danych karty kredytowej i obciążenia jej kwotą 2 złotych przekazywaną na cele charytatywne. Inny sposób potwierdzenia tożsamości konta rodzica to przesłanie zeskanowanych dokumentów.

WŁĄCZAMY MONITOROWANIE AKTYWNOŚCI DZIECKA ONLINE

1 Wchodzimy na stronę **account.microsoft.com/family** i klikamy na **Aktywność** przy profilu dziecka wśród członków rodziny.

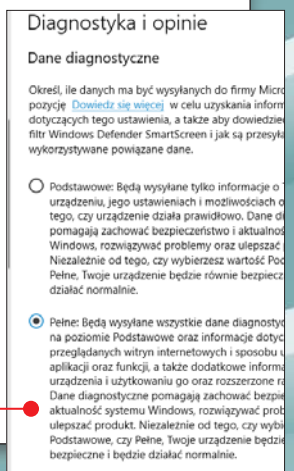
2 Otworzy się okno konfiguracji aktywności. Tam w sekcji **Pilnuj dzieci w Internecie** należy przestawić na **Włączone** przełącznik przy opcji **Raportowanie aktywności**.





Informacje o aktywności są zbierane z urządzeń z systemem Windows 10, konsoli Xbox One i urządzeń z systemem Android (w wersji minimum 5.0) z aplikacją Microsoft Launcher, w których do logowania używane jest konto dziecka. Informacje mogą być wysyłane do rodzica na przykład w formie cotygodniowego podsumowania dostarczanego e-mailem.

3 Aby funkcja raportowania aktywności działała, potrzebujemy odpowiednich ustawień prywatności na urządzeniu dziecka. W systemie Windows 10 otwieramy **Ustawienia**, klikamy na **Prywatność** oraz na **Opinie i diagnostyka** i upewniamy się, że ustawiono poziom **Pełne**.



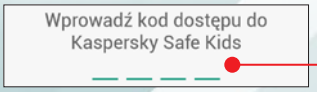
ELSKA NA DWA SPOSOBY

KASPERSKY SAFE KIDS

Kaspersky Safe Kids (DVD-KOD: **023**) to kompleksowe rozwiązanie do kontroli rodzicielskiej – zestaw aplikacji, które możemy zainstalować na komputerach z Windows, komputerach Mac, iPhone'ach, iPadach, a także urządzeniach z systemem Android. Na każdym z tych urządzeń aplikacje mogą pracować zarówno w trybie rodzica, jak i dziecka. Najlepszym rozwiązaniem dla rodzica jest zainstalowanie aplikacji w trybie rodzic na urządzeniu mobilnym, które mamy zawsze pod ręką. Możliwość śledzenia aktywności powiązana jest z zalogowaniem się do aplikacji Kaspersky Safe Kids poprzez wspólne konto **My Kaspersky**.

Jak zacząć

Po uruchomieniu aplikacji należy zalogować się lub zarejestrować. Dalej należy wybrać, w jakim trybie ma pracować urządzenie – wybieramy opcję **Rodzic**. Aby dziecko, mając w rękach telefon rodzica, nie mogło wyłączyć opcji kontroli rodzicielskiej, każda aktywność (bezpośrednio po wejściu do programu) musi być poprzedzona podaniem określonego przez nas kodu PIN.



KONFIGURACJA NA URZĄDZENIACH DZIECKA

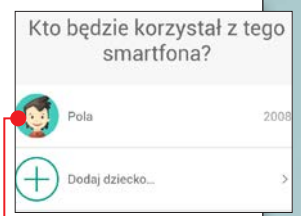
Aplikacja na komputery z Windows i komputery Mac wygląda podobnie. Nieco inaczej zaś w przypadku urządzeń mobilnych.

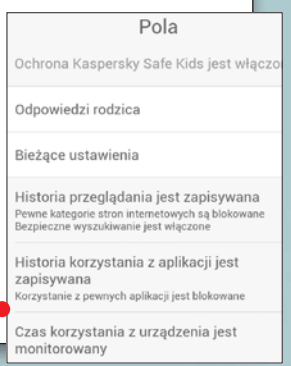
Na komputerze

Zacznijmy od komputerów. Po zainstalowaniu aplikacji logujemy się do niej przez to samo konto **My Kaspersky**, przez które logujemy się też na urządzeniu mobilnym. Wybieramy, że aplikacja ma pracować w trybie dziecka. Program pozwala na przypisanie oddzielnych ustawień dla każdego konta, na jakie logujemy się do komputera. Możemy stworzyć profil dziecka na koncie dziecka, a profil rodzica na swoim koncie. Po zalogowaniu na koncie dziecka tworzymy jego profil, podając imię dziecka i rok urodzenia (ma on wpływ na początkową konfigurację ograniczeń, ponieważ program może blokować aplikacje i strony internetowe).

Na urządzeniu mobilnym

Na urządzeniu mobilnym dziecka też instalujemy aplikację, logujemy się do niej przez konto **My Kaspersky** i wybieramy opcję **Dziecko**. Tu też możemy przypisać urządzenie do dziecka, a jeśli stworzyliśmy jego profil na innym urządzeniu, teraz możemy go tylko wybrać. Dziecko z poziomu aplikacji może sprawdzić, co jest monitorowane i do czego dostęp jest ograniczony.

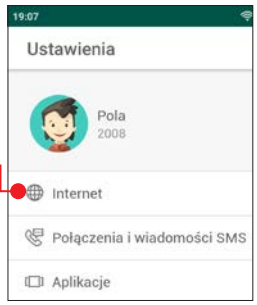


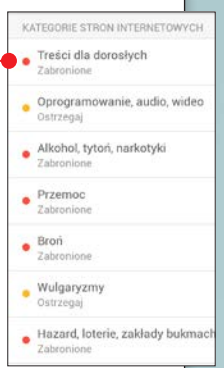


KONFIGURACJA OGRANICZEŃ I MONITOROWANIA DOSTĘPU DO INTERNETU W APLIKACJI RODZICA

W aplikacji mobilnej rodzica naciskamy przycisk z kołem zębatym, aby

przejść do ustawień. Są one podzielone na kategorie. W kategorii **Internet** możemy włączać lub wyłączać monitorowanie aktywności sieciowej dziecka, a także włączyć lub wyłączyć możliwość bezpiecznego wyszukiwania, by uniknąć wyświetlania stron internetowych z pornografią w wynikach wyszukiwania. Jest tu też zestawienie kategorii stron internetowych. Po wybraniu jednej z nich możemy ustawić jej stan na **Dozwolone**, **Ostrzegaj** lub **Zabronione**. Jeśli dla kategorii **Oprogramowanie audio wideo** dziecko ma ustawioną opcję **Ostrzegaj**, gdy spróbuje wejść na stronę z materiałami audiowizualnymi (jak You Tube), w przeglądarce pojawi się ostrzeżenie, ale dziecko będzie mogło otworzyć stronę. Gdy jednak to zrobi, w aplikacji rodzica pojawi się powiadomienie.





TRIKI
DO SYSTEMU
MENEDŻER ZADAŃ

10 WSKAZÓWEK DO

*Kiedy Windows 10 lub 8 nie działa jak należy, **pomoże nam Menedżer zadań**. Narzędzie to pokaże, co spowalnia pracę komputera, i pozwoli zatrzymać programy odmawiające posłuszeństwa. Zobaczmy, jak z niego korzystać*

1 URUCHAMIANIE MENEDŻERA ZADAŃ PRZEZ IKONĘ SKRÓTU

Menedżer zadań najszybciej uruchomimy skrótem klawiaturowym ctrl + shift + esc. Możemy też w wyszukiwarkę systemową wpisać **menedżer** lub krócej – **task**. Po uruchomieniu Menedżera zadań warto kliknąć na **Więcej szczegółów** u dołu okna.
Aby ułatwić sobie włączanie Menedżera zadań, dobrze jest przypiąć jego ikonę do paska zadań. W tym celu po otworzeniu go klikamy prawym przyciskiem myszy na jego ikonę na pasku i wybieramy **Przypnij do paska zadań**. Można także od razu w wyszukiwarce systemowej kliknąć w wynikach na **Menedżer zadań** prawym przyciskiem myszy i wskazać **Przypnij do paska zadań**.

2 WYKRYWANIE I ROZWIĄZYWANIE PROBLEMÓW Z WYDAJNOŚCIĄ

W oknie Menedżera zadań zobaczymy i zatrzymamy aplikacje nadmiernie obciążające komputer oraz programy zawieszone. Na zakładce **Procesy** zobaczymy wszystkie pracujące programy i funkcje Windows, także te pracujące w tle. Jeśli klikniemy na nagłówek kolumny **Procesor CPU**, zobaczymy u góry te, które najbardziej obciążają procesor. Kliknięciami na nagłówki kolumn **Pamięć**, **Dysk** i **Sieć** wyświetlimy najżarłoczniejsze aplikacje w danej kategorii. Programy nieodpowiadające na nasze polecenia (zawieszone) najłatwiej znajdziemy, sortując je alfabetycznie – wystarczy kliknąć na kategorię **Nazwa**. Aby wyłączyć taki program, klikamy na jego nazwę i u dołu po prawej stronie na **Zakończ zadanie**.

Nazwa	5% Procesor CPU	84% Pamięć	0% Dysk	0% Sieć
Adobe InDesign CS6 (32-bitowy)	2,2%	312,2 MB	0 MB/s	0 Mb/s
WMI Provider Host	1,1%	12,8 MB	0 MB/s	0 Mb/s
Menedżer okien pulpitu	0,8%	41,2 MB	0 MB/s	0 Mb/s
Microsoft Edge	0,3%	67,4 MB	0 MB/s	0 Mb/s
Menedżer zadań	0,3%	16,9 MB	0 MB/s	0 Mb/s
Firefox	0,2%	137,0 MB	0 MB/s	0 Mb/s
Firefox	0,2%	159,6 MB	0 MB/s	0 Mb/s
Host usługi: Instrumentacja zarządzania Windows	0,2%	14,0 MB	0 MB/s	0 Mb/s

3 PRZYZNAWANIE PROGRAMOWI WIĘKSZEJ WYDAJNOŚCI

Menedżer zadań pozwala wprowadzić takie ustawienia, by dany program aż do kolejnego ponownego uruchomienia peceta miał więcej mocy. W tym celu klikamy na wybrany program prawym przyciskiem myszy i wybieramy **Przejdź do szczegółów**, klikamy prawym przyciskiem myszy na zaznaczony proces i wybieramy **Ustaw priorytet**, a potem na przykład – **Wysoki**. Klikamy na **Zmień priorytet**.

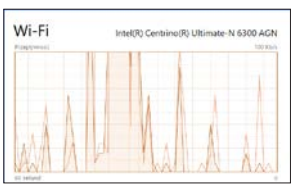
4 REANIMACJA WINDOWS

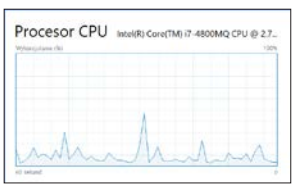
W razie zawieszenia Windows często pomaga taki trik: na zakładce **Procesy** klikamy prawym przyciskiem myszy na **Eksplorator Windows** i na **Uruchom ponownie**, i to wszystko! Jeśli nie można otworzyć Menedżera zadań, klikamy przy wciśniętych klawiszach ctrl + shift prawym przyciskiem myszy na wolne miejsce paska zadań i wybieramy **Zakończ pracę Eksploratora**. Znikną wtedy wszystkie okna i menu. Następnie naciskamy ctrl + shift + esc, by uruchomić Menedżer zadań. W jego oknie klikamy na **Więcej szczegółów** (jeśli trzeba). Klikamy na **Plik**, **Uruchom nowe zadanie**, wpisujemy **explorer** i klikamy na **OK**.

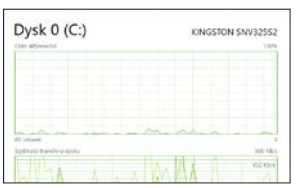
MENEDŻERA ZADAŃ

5 PRZEGLĄD **INFORMACJI O KOMPUTERZE**

W Menedżerze zadań możemy kontrolować informacje dotyczące wydajności komputera. Na zakładce **Wydajność** po kliknięciu z lewej strony na **CPU** widzimy obciążenie procesora. Możemy też kliknąć na **Pamięć**, **Dysk** i ewentualnie na **GPU** (karta graficzna), by obserwować obciążenie tych komponentów sprzętowych w czasie rzeczywistym. Transmisję danych z komputera możemy kontrolować, klikając na **Ethernet**, **Wi-Fi** albo **Wi-Fi** i **Bluetooth**. Wszystkie wykresy możemy zminimalizować i rozmieścić dowolnie na pulpicie. Jeśli na przykład chcemy mieć na oku obciążenie sieci Wi-Fi, klikamy na **Wi-Fi** i dwukrotnie na wyświetlony wykres. Ponowne podwójne kliknięcie zamyka widok kompaktowy.







6 PRZYSPIESZANIE **URUCHAMIANIA KOMPUTERA**

Wiele programów startuje razem z Windows i spowalnia uruchamianie komputera. Po kliknięciu na zakładkę **Uruchamianie** zobaczymy w kolumnie **Wpływ na uruchamianie**, w jakim stopniu spowalniają uruchamianie systemu. Aby wyłączyć program z autostartu Windows, klikamy na niego prawym przyciskiem myszy i wybieramy **Wyłącz**. Aby go ponownie włączyć, klikamy na **Włącz**. Możemy poeksperymentować, ale pamiętajmy, by nie wyłączać z autostartu programów potrzebnych od momentu włączenia komputera, jak choćby ochrona antywirusowa.

7 BADANIE **PODEJRZANYCH PROCESÓW**

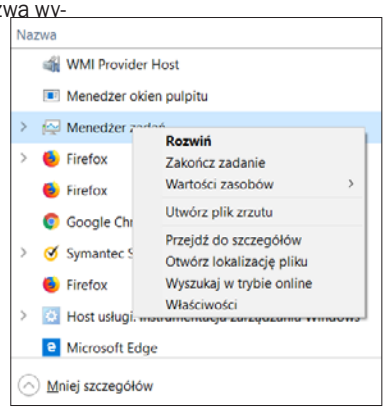
Niektóre działające procesy mają niezrozumiałe nazwy. Jeśli jeden z nich wydaje się nam podejrzany, to Menedżer zadań pomoże nam go sprawdzić.

Szukanie informacji w internecie

Sprawdźmy w internecie, co kryje się za nazwą wybranego programu. Wystarczy na niego kliknąć prawym przyciskiem myszy i wybrać **Wyszukaj w trybie online**. Menedżer zadań wyszuka daną nazwę w wyszukiwarce Bing w naszej domyślnej przeglądarce.

Otwieranie folderu programu

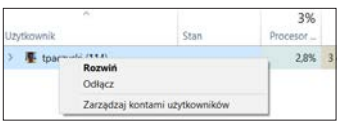
Informacji o programie może dostarczyć także jego lokalizacja. Aby ją poznać, klikamy prawym przyciskiem myszy na aplikację i wybieramy **Otwórz lokalizację pliku**. Otworzy się folder z plikiem programu.



KRÓTKIE WSKAZÓWKI **DO MENEDŻERA ZADAŃ**

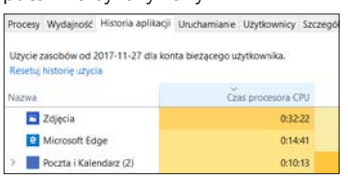
8 WYLOGOWANIE UŻYTKOWNIKA

Jeżeli inni użytkownicy Windows są zalogowani na tym samym komputerze, to aktualny użytkownik nie może ich wylogować. Można to natomiast zrobić w Menedżerze zadań: klikamy na **Użytkownicy**, prawym przyciskiem myszy na wybrane konto Windows, na **Odłącz** i na **Odłącz użytkownika**.



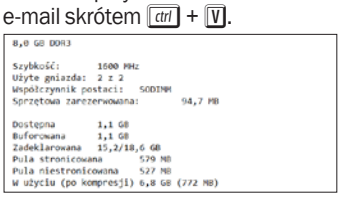
9 JAK DŁUGO PRACUJE PROGRAM

Najczęściej używane aplikacje wbudowane w Windows zobaczymy na zakładce **Historia aplikacji** w kolumnie **Czas procesora CPU**. W wypadku tradycyjnych programów klikamy na zakładkę **Szczegóły**, prawym przyciskiem myszy na nagłówek kolumny **Nazwa**. Wybieramy **Wybierz kolumny**, zaznaczamy **Czas procesora CPU** i zatwierdzamy, klikając na **OK**. Teraz po kliknięciu na **Czas procesora CPU** zobaczymy najaktywniejsze programy. Na marginesie: pozycję **Proces bezczynności systemu** możemy zignorować, bo pokazuje, jak długo komputer nie był używany.



10 KOPIOWANIE INFORMACJI O PECECIE

Chcemy wysłać znajomemu informację o naszym sprzęcie? Klikamy na **Wydajność**, a potem na wybraną pozycję, jak **CPU** czy **Pamięć**. Naciskamy Ctrl + C. Skopiowane informacje trafiają do schowka – możemy je wkleić na przykład do wiadomości e-mail skrótem Ctrl + V.



TRIKI
DO SYSTEMU
WERSJA WINDOWS DO ZADAŃ SPECJALNYCH

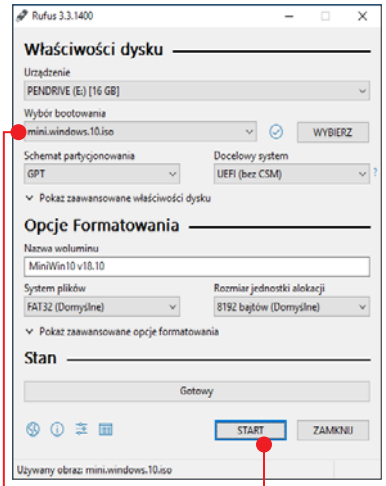
MEDICAT I WIN PE –

Oto zestaw ratunkowy, który pomoże nam w problemach z komputerem. ***Pakiet MediCat USB zawiera wiele narzędzi, jak na przykład skanery antywirusowe, a także Win PE****, specjalną przedinstalacyjną wersję Windows*

Środowiska ratunkowe, jak **MediCat USB z Win 10 PE**, mogą działać jak wersje Live systemów operacyjnych. Uruchamiamy je z nośników jak płyta DVD lub pendrive. Dane wczytywane są do pamięci komputera i środowisko zostaje uruchomione. Dzięki temu, nawet jeśli korzystamy z mało wydajnego nośnika, będziemy mogli sprawnie pracować. Win PE to system ratunkowy, który działa w trybie Wiersza polecenia – poprzez specjalne komendy pozwala na ratowanie Windows, który przestał się uruchamiać. Ma zresztą znacznie szersze możliwości (o tekstowym Win PE więcej przeczytamy w poradniku PDF do pobrania z KŚ+). Jest jednak trudny w obsłudze. I tu z pomocą przychodzi zestaw MediCat USB – tworzony jako nowoczesny następca nierozwijanego już Hiren's Boot Disk. MediCat USB zawiera mnóstwo dodatkowych narzędzi i zintegrowane środowisko Win PE wyposażone w przyjazny interfejs graficzny. Jest pulpit, są ikony, możemy nawet skorzystać z przeglądarki internetowej wbudowanej w MediCat USB. Wybór narzędzi pomocnych przy ratowaniu komputera jest duży, a mamy też dostęp do ogromnej biblioteki aplikacji typu portable – czyli działających bez potrzeby instalacji. **kd**

TWORZYMY BOOTOWALNY NOŚNIK Z MEDICAT

Obraz systemu w formacie ISO pobieramy z **KŚ+ (www.ksplus.pl)**. Następnie możemy wypalić go na DVD lub stworzyć specjalny pendrive z systemem. Polecana jest ta druga opcja, ponieważ nośniki USB są szybsze niż DVD. W naszym przykładzie wykorzystamy program **Rufus** (DVD-KOD: **052**), który służy do tworzenia takich nośników.

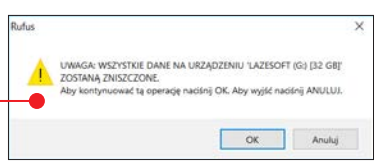


1 Podłączamy nośnik USB do komputera, a potem uruchamiamy program Rufus.

2 Klikamy na **Wybierz** i wskazujemy lokalizację pliku z obrazem systemu.

3 Po weryfikacji obrazu klikamy na **Start**.

4 Następnie wyrażamy zgodę na **usunięcie wszystkich danych z nośnika** i potwierdzamy wszystkie następne komunikaty.



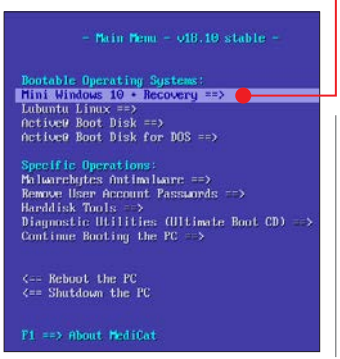
5 Po chwili bootowalny nośnik będzie gotowy. Uruchamiamy ponownie komputer i zmieniamy ustawienia bootowania tak, aby komputer włączył się, korzystając z pendrive'a.

URUCHAMIAMY SYSTEM MEDICAT

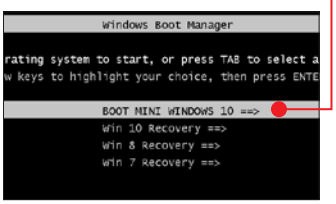
1 Gdy uruchomimy nasz komputer, wykorzystując bootowalny nośnik, pojawi się ekran startowy MediCat.

2 Po ekranie startowym poruszamy się za pomocą klawiatury. W pierwszym oknie wyrażamy zgodę, wybierając górną pozycję, i zatwierdzamy, wciskając klawisz enter.

3 W kolejnym oknie będziemy mogli wybrać system, który chcemy uruchomić. W naszym przykładzie wybieramy **Mini Windows 10 + Recovery**.



4 Następnie wskazujemy opcję **BOOT MINI WINDOWS 10** i wciskamy enter.

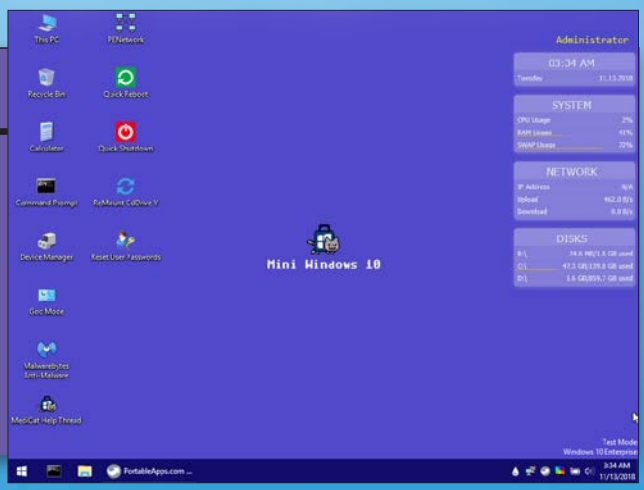


5 Wszystkie pliki zostaną załadowane do pamięci komputera i po chwili uruchomiony zostanie specjalny ratunkowy system operacyjny.

ZESTAW RATUNKOWY

KORZYSTAMY Z MEDICAT

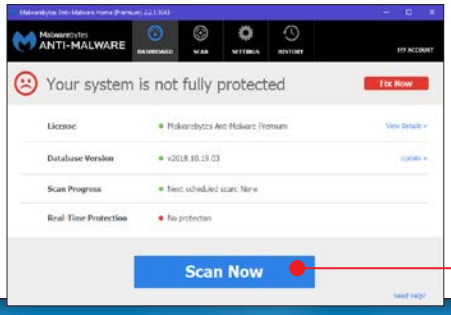
Interfejs samego systemu jest bardzo zbliżony do tego znanego nam z Windows. Na dole ekranu znajdziemy menu Start i pasek zadań, a na pulpicie podstawowe narzędzia, które mogą się nam przydać w ratowaniu komputera, między innymi skaner Malwarebytes Anti-Malware. Uruchamiając Wiersz polecenia, będziemy mieli dostęp do typowego interfejsu Win PE. Po prawej stronie ekranu znajdziemy specjalny widget, który informuje nas o parametrach pracy naszego komputera. Jednak jeden z najbardziej przydatnych elementów tego środowiska znajdziemy w zasobniku systemowym – jest to aplikacja PortableApps, która pozwala uzyskać dostęp do wielu różnych programów i uruchamiać je w środowisku ratunkowym. Do poprawnego działania PortableApps wymagany jest dostęp do internetu.

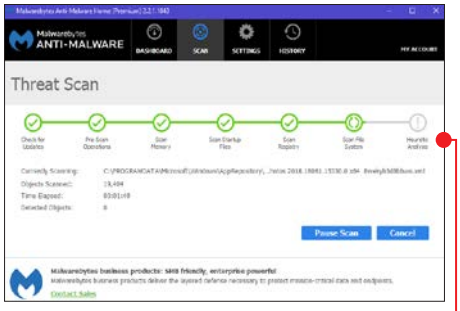


SKANUJEMY KOMPUTER W POSZUKIWANIU ZAGROŻEŃ

1 Na pulpicie MediCat znajdziemy skrót do programu **Malwarebytes Anti-Malware**. Klikamy na niego dwukrotnie.

2 Następnie klikamy na **Scan Now** u dołu ekranu.





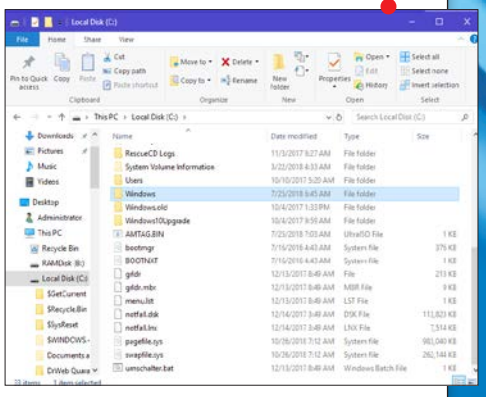
3 Po chwili nasz komputer zostanie przeskanowany. Jeśli program znajdzie jakieś zagrożenia, wyświetli o nich informacje i pozwoli nam podjąć decyzję, czy ma je usunąć, czy przenieść do kwarantanny. Na koniec wystarczy kliknąć na **Finish**.

KOPIUJEMY WAŻNE PLIKI

Dzięki MediCat możemy uzyskać dostęp do danych na naszych dyskach, nawet jeżeli system Windows się nie uruchamia. Jeśli podłączymy dodatkowy nośnik USB, na przykład dysk zewnętrzny, będziemy mogli wygodnie przekopiować ważne dla nas dane, których nie chcemy stracić.

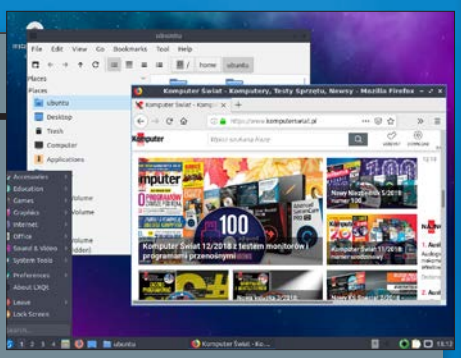
1 Klikamy na pasku zadań na ikonę **Eksploratora plików**.

2 Następnie nawigujemy do plików, które chcemy przekopiować, i przenosimy je do wybranego przez nas miejsca.



LINUX NA WSZELKI WYPADEK

Jeśli chcemy, możemy również uruchomić dostępną w pakiecie wersję Live systemu Lubuntu. Dzięki niemu będziemy mogli korzystać z w pełni funkcjonalnego systemu, a dodatkowo uzyskamy również dostęp do danych na naszych dyskach lokalnych. Wystarczy, że w **Boot Menu** wybierzemy opcję **Lubuntu Linux** i wciśniemy enter, a później tak samo zatwierdzamy wybór opcji **Start Lubuntu**.



TRIKI DO SYSTEMU
APLIKACJA TWÓJ TELEFON

POŁĄCZENIE S

Z ANDROIDEM LUB IOS Z KOMPUTEREM

*Smartfon to właściwie mały komputer. Dzięki nowej funkcji Windows 10 możemy **wygodnie kontynować na smartfonie pracę** zaczętą na komputerze i odwrotnie, a także **wysyłać SMS-y z komputera**. Zobaczmy, jak to robić*

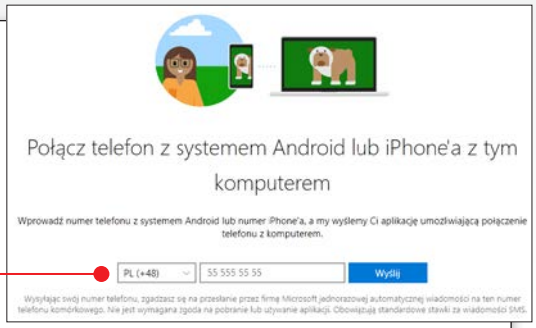
Najnowsza wersja systemu Windows 10 wyposażona została w funkcję **Twój telefon** i aplikację o tej samej nazwie, która pozwala nawiązać kontakt z urządzeniem mobilnym. Po dodaniu do systemu Windows 10 naszego telefonu z Androidem (lub iOS) możemy przeglądać pliki multimedialne ze smartfona na komputerze, a także wysyłać SMS-y bezpośrednio z komputera. Możliwe jest też kontynuowanie na komputerze przeglądania internetu, które rozpoczęliśmy na smartfonie w przeglądarce Edge. **kż**

ŁĄCZYMY TELEFON Z KOMPUTEREM

By przedstawiona wskazówka zadziałała, oba urządzenia muszą być połączone z tą samą siecią lokalną. Powinniśmy być też zalogowani do konta Microsoft.

1 Uruchamiamy ustawienia systemowe, przechodzimy do sekcji **Telefon**. Klikamy na **Dodaj telefon**, a potem na **Kontynuuj**.

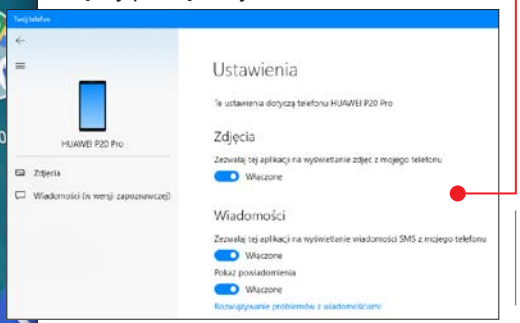
2 Klikamy na **Połącz telefon**. W kolejnym oknie wpisujemy numer naszego telefonu i klikamy na **Wyślij**. Na smartfon wysłany zostanie link do narzędzia **Pomocnik aplikacji Twój telefon**. Możemy je też pobrać bezpośrednio z Google Play.



3 Po zainstalowaniu Pomocnika aplikacji Twój telefon wybieramy **Zaloguj się przy użyciu konta Microsoft**. Wyświetli się prośba o nadanie uprawnień do łączenia z komputerem. Wybieramy **Zezwalaj**. Potwierdzamy też systemowe żądania o uprawnienia – jeśli ich nie nadamy na przykład dla SMS-ów, nie będzie możliwe wysyłanie SMS-ów z komputera.

APLIKACJA TWÓJ TELEFON

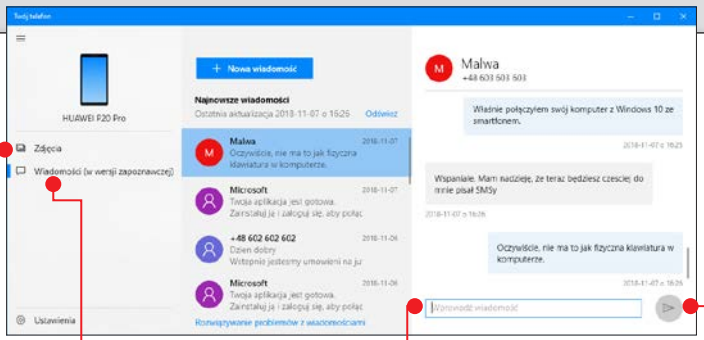
1 By uruchomić Twój telefon, w menu Start wybieramy **Ustawienia** i **Telefon** (lub wyszukujemy nazwę **Twój telefon** w wyszukiwarce systemowej). Po uruchomieniu wyświetli się okno, w którym możemy przełączać się pomiędzy podłączonymi telefonami.



2 Wybieramy nasz telefon i klikamy na **Ustawienia**. Aktywujemy suwakami wszystkie opcje.

3 Klikamy na **Zdjęcia**, by obejrzeć ostatnie obrazy utworzone na smartfonie. Klikając na miniaturę, otworzymy dany plik w domyślnej przeglądarce grafiki Windows 10.

4 By wysłać SMS z komputera w aplikacji Twój telefon, klikamy na **Wiadomości**, a potem **Wyślij powiadomienie**. Jeśli wcześniej przyznaliśmy uprawnienia, nie musimy nic robić na smartfonie.



5 W oknie **Twój telefon** wyświetli się lista wątków SMS-owych. Podobnie jak w smartfonie klikamy na wybrany, by kontynuować rozmowę. Tekst wpisujemy w pole i wysyłamy, klikając na przycisk.

6 Jeśli chcemy wysłać nowy SMS, klikamy na **Nowa wiadomość**. Wpisujemy numer lub nazwę kontaktu i wciskamy enter, by rozpocząć konwersację.

MARTFONA

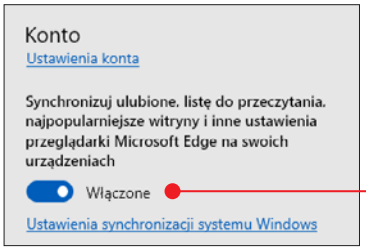
Z WINDOWS 10

OGRANICZENIA APLIKACJI TWÓJ TELEFON

Narzędzie Twój telefon dla Windows 10 jest w fazie rozwojowej i będą do niego z czasem dodawane kolejne funkcje. Obecnie przeglądanie zdjęć ograniczone jest do 25 ostatnich obrazów (zarówno zdjęć, jak i zrzutów ekranu), dlatego najlepiej nadaje się ono do pracy nad nowymi plikami.
Funkcja przesyłania wiadomości nie obsługuje na razie komunikacji poprzez MMS, a także kopiowania całości konwersacji do schowka.

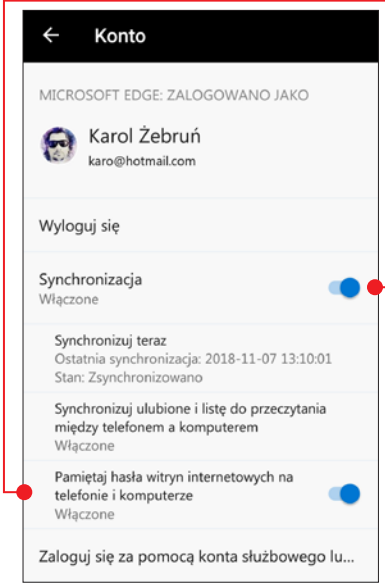
MICROSOFT EDGE – SYNCHRONIZACJA USTAWIEŃ

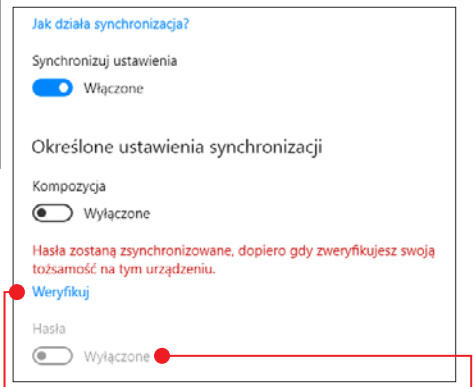
Wśród ustawień, które możemy synchronizować pomiędzy urządzeniami, najważniejsze są hasła. Edge domyślnie ofertuje zapisywanie haseł, trzeba jednak wymusić ich synchronizację.



1 W przeglądarce klikamy na trzy kropki w prawym górnym rogu okna i wybieramy **Ustawienia**. Na zakładce **Ogólne** aktywujemy suwak. By synchronizacja zadziałała, musimy być zalogowani do naszego konta Microsoft.

2 W smartfonie po uruchomieniu Edge logujemy się na nasze konto Microsoft. Również naciskamy ikonę menu, a potem **Ustawienia**. W sekcji **Konta** wybieramy nazwę konta, a potem aktywujemy ustawienie, a także, by synchronizować hasła do kont i witryn. Synchronizację wymusimy od razu, wybierając **Synchronizuj teraz**.



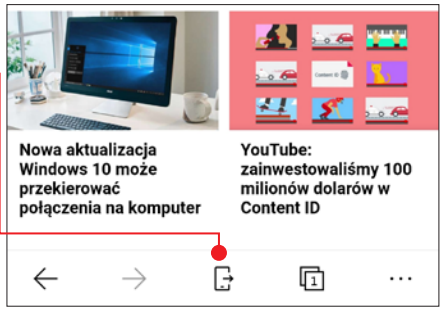


3 Może być konieczne zweryfikowanie dostępu do konta. W smartfonie postępujemy według instrukcji na ekranie. W komputerze klikamy na **Ustawienia konta**, a potem na **Weryfikuj**. Po pomyślnej weryfikacji możemy aktywować suwak **Hasła**.

MICROSOFT EDGE – KONTYNUACJA PRACY

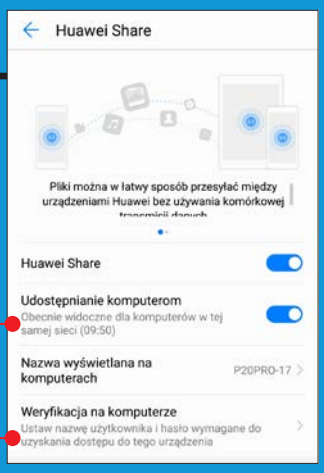
1 W przeglądarce Edge na smartfonie wybieramy. Wyszukane zostaną urządzenia w pobliżu powiązane z naszym kontem Microsoft.

2 Wskazujemy komputer na liście urządzeń i po chwili w oknie Edge na tym urządzeniu pojawi się strona, którą przeglądaliśmy właśnie na smartfonie.



DOSTĘP DO ZAWARTOŚCI SMARTFONA

Oprócz narzędzi systemu Windows 10 dostęp do zawartości smartfona umożliwiają dedykowane narzędzia oferowane przez producentów. Niektóre smartfony mają też systemową opcję, która zapewnia współdzielenie zawartości, na przykład **Huawei Share** w przypadku smartfonów marki Huawei. Po jej aktywowaniu w ustawieniach tego narzędzia możemy zezwolić na dostęp do pamięci smartfona jako zasobu sieciowego (wymagane są dane logowania ustawiane w).



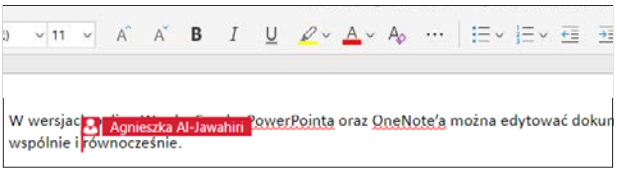
TRIKI
DO PROGRAMU
OFFICE ONLINE

WSKAZÓWEK DO

Pakiet biurowy Microsoftu jest dostępny jako program na pecet, ale też jako ***wersja przeglądarkowa oraz aplikacja mobilna*** *– bezpłatnie! Oto najlepsze wskazówki*

1 WSPÓLNA EDYCJA DOKUMENTU

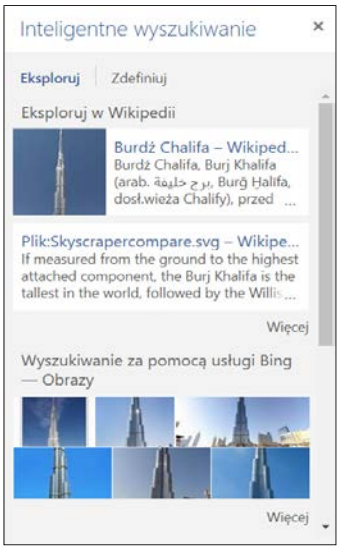
W wersjach online Worda, Excela, PowerPointa oraz OneNote'a można edytować dokumenty wspólnie i równocześ nie. Aby pracować w zespole, nasi współpracownicy nie muszą nawet mieć konta Microsoft. Dzięki widokowi w czasie rzeczywistym każdy od razu zobaczy teksty albo zdjęcia dodawane przez innych użytkowników. Aby zacząć pracę, w przeglądarce otwieramy stronę **office.com** i logujemy się. Wybieramy aplikację pakietu Office, na przykład Worda. Następnie klikamy na jeden z gotowych szablonów dokumentu lub na **Nowy pusty dokument**. Możemy też otworzyć jeden z edytowanych ostatnio dokumentów z listy **Ostatnio używane**. W trybie edycji klikamy na **Udostępnij** i podajemy adresy e-mail współpracowników. U dołu okna z listy możemy wybrać **Adresaci mogą edytować** lub **Adresaci mogą tylko wyświet lać** Po kliknięciu na **Udostępnij** i na **Zamknij** nasi współpracownicy otrzymają wiadomość e-mail z linkiem. Po kliknięciu na niego dokument otworzy się w przeglądarce w aplikacji Word Online.



Podczas współpracy zawsze dokładnie będziemy wiedzieć, w którym miejscu dokumentu aktualnie są wprowadzane zmiany

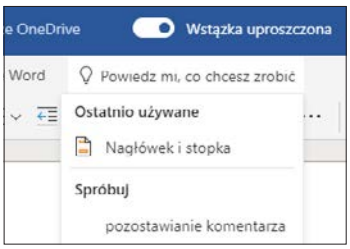
2 SZYBKIE I INTELIGENTNE WYSZUKIWANIE

Jeśli w dokumencie pojawia się pojęcie, którego znaczenia nie znamy, to **Word Online** nie zostawi nas bez pomocy. Zaznaczamy myszą problematyczną część tekstu, klikamy na nią prawym przyciskiem myszy i wybieramy **Inteligentne wyszukiwanie**. Po prawej stronie dokumentu pojawi się kolumna z informacjami, wyjaś nieniami izdjęciami wyszukanymi przez wyszukiwarkę Bing. Jeśli potrzebujemy dokładniejszych wyjaśnień, możemy kliknąć na link do Wikipedii.



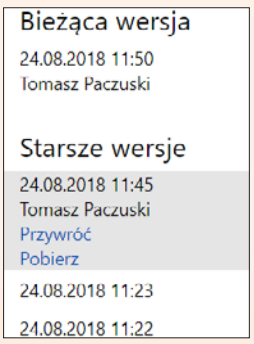
3 SZYBSZE WYKRYWANIE FUNKCJI

Wszystkie aplikacje pakietu **Office Online** mają praktycznego asystenta, który szybko wywołuje potrzebne funkcje. Klikamy u góry okna na pole **Powiedz mi, co chcesz zrobić** i wpisujemy, co jest nam potrzebne, na przykład **Nagłówek**. Zobaczymy listę poleceń oraz tematów pomocy pasujących do wpisanego hasła – wybieramy je kliknięciami. To wygodniejsze niż poszukiwanie potrzebnych funkcji w menu.

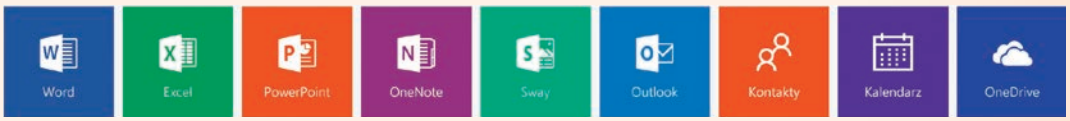


4 PRZYWRACANIE STARYCH WERSJI

Pracujemy pilnie nad dokumentem i po pewnym czasie zauważamy, że trochę nabałaganiliśmy. Nic się nie stało. Office Online automatycznie cały czas zapisuje dokumenty i zachowuje ich poprzednie wersje. Aby przywrócić wcześniejszy stan dokumentu, klikamy na **Plik**, **Informacje** i **Poprzednie wersje**. Pojawi się lista wszystkich wersji posortowana według dat i godzin. Kliknięcie na wybraną pozycję otwiera podgląd. Jeśli chcemy przywrócić daną wersję, klikamy na **Przywróć**.



Office ONLINE



5 OFFICE MULTITASKING NA TABLECIE APPLE

Na telefonie i tablecie także możemy czytać dokumenty Worda albo dopracowywać prezentację PowerPointa. W mobilnej przeglądarce jest to jednak dość karkołomne, lepiej robić to w aplikacjach – programy pakietu Office możemy pobrać w darmowych wersjach dla iOS oraz Androida. **Uwaga!** W wypadku tabletów z przekątną ekranu powyżej 10,1 cala, jak na przykład duży iPad Pro, do korzystania z aplikacji potrzebny jest płatny abonament Office 365. Dla mniejszych urządzeń oprogramowanie jest bezpłatne. Jeszcze jedna wskazówka dla użytkowników iPadów: począwszy od iOS 11 funkcja drag & drop jest możliwa także pomiędzy programami Microsoft Office. Otwieramy pierwszą aplikację, na przykład Worda. Potem przeciągamy od dołu, aby otworzyć dock, i przeciągamy do góry drugą aplikację, na przykład OneDrive. Ta pojawi się teraz w widoku Slide Over, a więc jako aplikacja szybująca nad aktualnym widokiem. Nowsze iPady (od Air 2) oferują oprócz tego Split View (patrz zdjęcie), w którym dwa programy rozmieszczone obok siebie dzielą ekran. Aby przenieść element, dotykamy na przykład zdjęcia zapisanego w chmurze, przytrzymujemy na nim palec i przeciągamy do wybranego miejsca dokumentu Worda.

6 PREZENTACJE INACZEJ

Najnowszym programem pakietu Office jest narzędzie do prezentacji Sway. Inaczej niż w PowerPoincie nie wypełniamy w nim slajdów, tylko tworzymy cyfrowy magazyn. Klikamy na **Utwórz nowy** lub na szablon, na przykład **Opowieść wakacyjna**, aby stworzyć zdjęciowy zapis podróży. Kliknięciem na **Rozpocznij edytowanie tego Swaya** przechodzimy do edycji. Klikając na poszczególne elementy, zmieniamy teksty i zdjęcia. Nowe obiekty dodajemy, klikając na **+**. Elementy można chwytać za ramkę, by zmieniać ich kolejność. Aby zobaczyć podgląd (patrz zdjęcie po prawej stronie), klikamy na zakładkę **Projektowanie**. Klikając na **Style** w prawym górnym rogu (w widoku Projektowanie), zmienimy wygląd prezentacji. Klikając na **Scenariusz**, wracamy do edycji. Zapis jest automatyczny. Klikając na **Udostępnij**, wyślemy prezentację znajomym.

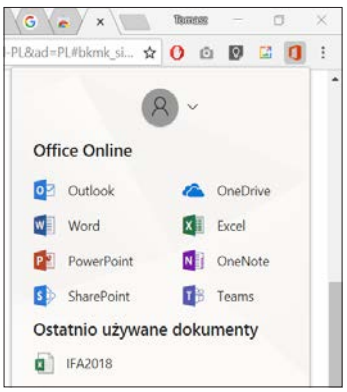
KRÓTKIE WSKAZÓWKI DO OFFICE ONLINE

7 POGAWĘDKI PODCZAS PRACY

Jeśli edytujemy ze współpracownikami na przykład dokument Worda (patrz wskazówka **1**), możemy z nimi pogawędzić podczas pracy. Klikając na ikonę czatu albo Skype'a, otworzymy pasek boczny. Aby rozpocząć w nim rozmowę, wybieramy kontakt i w pole u dołu wpisujemy wiadomość.

8 SZYBKI DOSTĘP

W przeglądarce dwoma kliknięciami otworzymy aplikację Office Online oraz ostatnio używane dokumenty. Niezbędne rozszerzenie (Office Online) jest dostępne wyłącznie dla Chrome i można je pobrać ze strony **chrome.google.com/webstore**. Kliknięcie na nową ikonę obok paska adresu otwiera okno wyboru.



TRIKI DO PROGRAMU *ONEDRIVE*

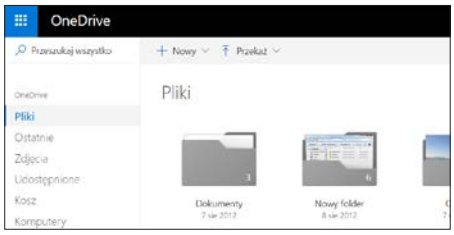
1 WSKAZÓWEK DO

1 CO JEST POTRZEBNE DO ONEDRIVE

- **Windows 8/10:** tutaj OneDrive jest preinstalowany. Musimy tylko zalogować się na koncie Microsoft.
- **Windows 7:** wymaga instalacji aplikacji OneDrive ze strony onedrive.live.com/about/pl-PL/download/
- **Android/iOS:** darmowe aplikacje są dostępne w sklepach Google Play i App Store.

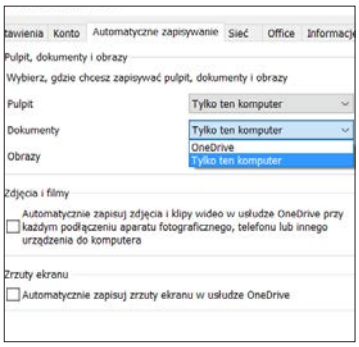
Tak wyślemy dane do chmury

Jeśli jesteśmy już zalogowani, naciskamy w komputerze równocześnie ⊞+E i kliknięciem na **OneDrive** otwieramy folder **OneDrive**. Kopiujemy do niego poszczególne pliki albo całe foldery. Teraz z każdego urządzenia połączonego z internetem możemy je otworzyć na stronie **onedrive.live.com** i w razie potrzeby pobrać. W aplikacji OneDrive na telefonie działa to podobnie.



2 AUTOMATYCZNE PODWÓJNE ZAPISYWANIE DOKUMENTÓW

Nikt nie może ze stuprocentową pewnością wykluczyć awarii twardego dysku. Dlatego bezpiecznie jest zapisywać dokumenty nie tylko na własnej pamięci masowej, ale dodatkowo także w OneDrive. Na życzenie nasze dokumenty Worda, arkusze Excela, PDF-y i inne pliki będą zapisywane podwójnie w sposób całkowicie automatyczny. Dzięki temu w dowolnym momencie będziemy mieli do dyspozycji ich kopie bezpieczeństwa.

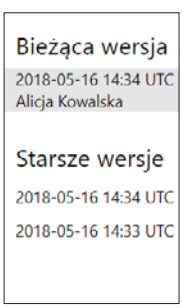


1 Klikamy prawym przyciskiem myszy u dołu po prawej stronie paska zadań na ikonę OneDrive i klikamy na **Ustawienia**.

2 Na karcie **Automatyczne zapisywanie** przy pozycji **Dokumenty** wybieramy **OneDrive** i zatwierdzamy zamiany przyciskiem **OK**.

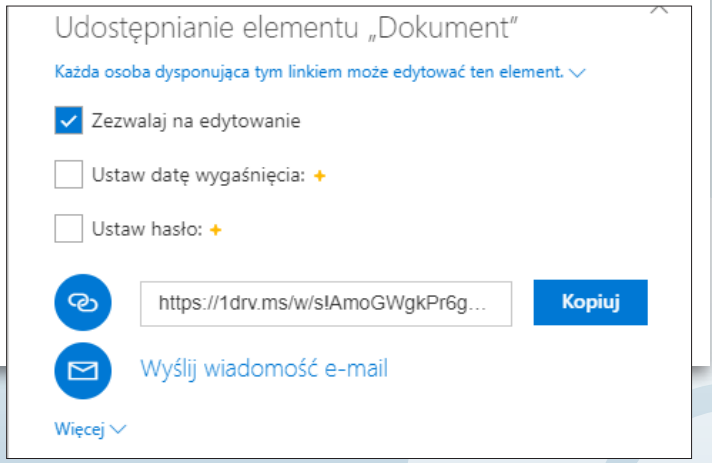
3 OTWIERANIE STARYCH WERSJI PLIKÓW

Jeżeli automatycznie zapisujemy dokumenty w OneDrive, jak opisano to we wskazówce **2**, to dodatkową korzyścią będzie dostęp do tak zwanej historii wersji. Jest to zapis nawet do 25 wersji danego dokumentu. To bardzo praktyczne, jeśli przez przeoczenie niepotrzebnie zapiszemy zmiany w dokumencie albo go skasujemy. Otwieramy stronę internetową **onedrive.live.com** i logujemy się za pomocą konta Microsoft. Przechodzimy do folderu (na ogół **Dokumenty**), w którym dokument jest zapisany. Klikamy na dokument prawym przyciskiem myszy i z menu wybieramy **Historia wersji**. Po lewej stronie pod **Starsze wersje** znajdziemy zapisane wcześniej wersje pliku.



4 UDOSTĘPNIANIE W ONEDRIVE ZAMIAST PRZESYŁANIA DUŻYCH PLIKÓW

Chcemy wysłać e-mail z dużym załącznikiem? Zamiast wielkiego pliku lepiej dołączyć link umożliwiający jego pobranie. Zaleta: wiadomość dotrze nawet wtedy, kiedy skrzynka odbiorcza adresata nie akceptuje dużych załączników. Zresztą wiadomości z załącznikami niepotrzebnie przepełniają skrzynkę odbiorczą. Oto jak to zrobić: kopiujemy plik do folderu OneDrive. Klikamy na niego prawym przyciskiem myszy i wybieramy **Udostępnij**. Chwilę później pojawi się okno udostępniania (patrz ilustracja). Klikamy na **Kopiuj link**. Otwieramy nasz program pocztowy lub komunikator, tworzymy nową wiadomość i wklejamy link, naciskając Ctrl+V i naciskamy spację. Odbiorca, by pobrać plik, musi tylko kliknąć na link, nie musi nawet logować się do OneDrive.

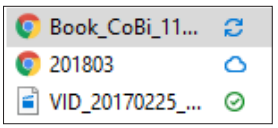


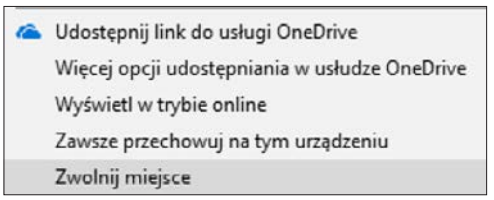
OneDrive

OneDrive stał się już pełnoprawnym komponentem Windows. *Przeczytajmy, jak wygodnie z niego korzystać, chronić nasze dane oraz jak najlepiej wykorzystać możliwości tego narzędzia*

5 PRZENOSZENIE POŻERACZY PAMIĘCI

Eksplorator plików wyświetla zawsze wszystkie pliki, nieważne, czy są zapisane lokalnie, czy w chmurze. Ikony obok pliku informują, gdzie fizycznie znajdują się poszczególne dane. Pliki dostępne tylko online rozpoznamy po chmurce. Jeśli plik jest dostępny także lokalnie, to obok niego pojawia się ikona z zielonym haczykiem. Niebieska podwójna strzałka informuje, że plik właśnie jest synchronizowany. W przypadku braku miejsca na dysku możemy skasować plik, pozostawiając go tylko w chmurze. Na wielu komputerach funkcja ta wymaga jednak włączenia. Oto jak to zrobić:





1 Klikamy prawym przyciskiem myszy na ikonę OneDrive na pasku zadań i na **Ustawienia**.

2 Na zakładce **Ustawienia** znajdujemy **Pliki na żądanie**. Opcja **Oszczędź miejsce…** musi być zaznaczona.

3 Aby skasować plik z dysku, pozostawiając go w chmurze, klikamy na niego prawym przyciskiem myszy i wybieramy polecenie **Zwolnij miejsce**.

6 SZYBSZE WYSYŁANIE

Jeśli często wysyłamy dużo plików do OneDrive, to może nam się przydać rozszerzenie polecenia **Wyślij do** w menu kontekstowym o pozycję OneDrive. Kiedy to zrobimy, pliki i foldery będziemy wysyłać do chmury tylko dwoma kliknięciami.

1 Naciskamy równocześnie ⊞+R, wpisujemy **shell:sendto** i naciskamy enter. Otworzy się Eksplorator plików z folderem **SendTo**.

2 Klikamy w nim prawym przyciskiem myszy na wolne miejsce i w menu kontekstowym wybieramy **Nowy** i **Skrót**. Następnie klikamy na **Przeglądaj**, **OneDrive**, **OK**, **Dalej** i na **Zakończ**.
To wszystko. Teraz wypróbujmy: klikamy na plik prawym przyciskiem myszy, wybieramy **Wyślij do** i **OneDrive**.
Kopia pliku wyląduje w folderze **OneDrive**.

7 POŻEGNANIE ZE SKANEREM: FOTOGRAFUJEMY DOKUMENTY

Aplikacja OneDrive dla iOS i Androida sprawia, że skanowanie dokumentów i wizytówek jest bardzo proste. Możemy zrezygnować z tradycyjnego skanera. W Androidzie robi się to tak: w aplikacji OneDrive dotykamy **+** i wybieramy **Skanuj**. Potem przytrzymujemy aparat nad dokumentem, aż zostanie on w całości objęty ramką. Dotykamy wyzwalacza, a w chwilę potem naciskamy **Gotowe** i **Przekaż**. Skan znajdziemy na pececie w folderze OneDrive w formacie PDF pod nazwą **Skan –….**

KRÓTKIE WSKAZÓWKI DO ONEDRIVE

8 CO SIĘ ZEPSUŁO: PECET CZY CHMURA

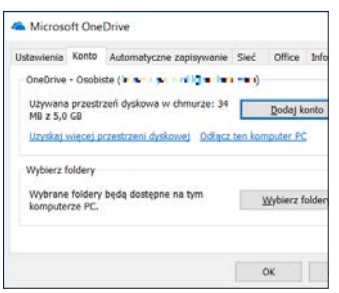
Jesteśmy wprawdzie online, ale OneDrive kwituje próbę dostępu do chmury komunikatem błędu? To zdarza się rzadko, niemniej może się zdarzyć.
Aby w takim przypadku wykluczyć defekt techniczny naszego peceta, odwiedźmy stronę **https://portal.office.com/servicestatus**. Tu od razu sprawdzimy, czy Microsoft ma problemy ze swoimi usługami online.

9 WYSYŁANIE ZDJĘĆ Z TELEFONU BEZPOŚREDNIO DO PECETA

Nasze zdjęcia z telefonu mogą być od razu widoczne na pececie. Uruchamiamy aplikację OneDrive (patrz wskazówka **1**), dotykamy **Ja**, **Ustawienia**, **Przekazywanie z aparatu**. Aby zmniejszyć zużycie energii w telefonie, możemy włączyć opcję **Przekazuj tylko przy ładowaniu**.
Zdjęcia z telefonu wylądują na naszym dysku w chmurze, a potem w folderze **OneDrive** na komputerze.

10 SPRAWDZANIE PAMIĘCI

Możemy łatwo sprawdzić, ile pamięci mamy jeszcze do dyspozycji w naszej chmurze OneDrive. Na komputerze otwieramy **Ustawienia** (patrz wskazówka **5**) i klikamy na zakładkę **Konto**.
W smartfonowej aplikacji dotykamy natomiast **Ja**.
Jeśli miejsca robi się mało, usuwamy niepotrzebne już pliki albo przechodzimy na odpłatną subskrypcję. Ceny rozpoczynają się od 1 TB za 30 złotych miesięcznie.



TRIKI DO PROGRAMU *OUTLOOK*

8 WSKAZÓWEK DO

Outlook to program pocztowy nie bez powodu często używany w firmach. Ma sporo ważnych zalet: pozwala podłączyć wiele adresów jednocześnie, synchronizować kontakty i kalendarze. Warto jednak poznać ***nieco bardziej ukryte funkcje*** *tego programu*

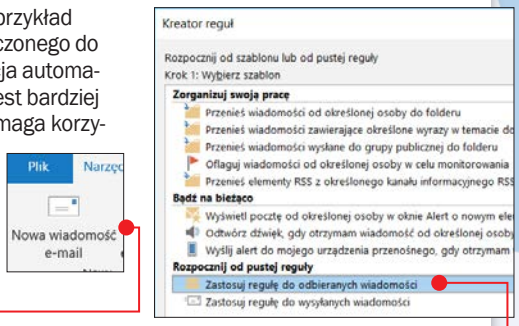
1 ŁATWA AUTOMATYCZNA ODPOWIEDŹ – TRYB URLOPU

Jeśli planujemy urlop lub nie będziemy przy komputerze przez kilka dni, warto ustawić opcję automatycznego odpowiadania do wszystkich nadawców. Dzięki temu osoby, które do nas napiszą, otrzymają od razu informację zwrotną o naszej nieobecności.

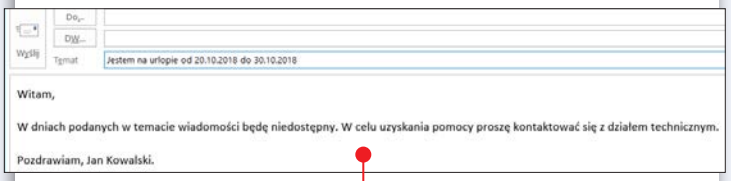
W wersji desktopowej wystarczy kliknąć na **Plik**, a potem na **Odpowiedź automatyczna** i postępować zgodnie z instrukcjami. W **Outlook.com** klikamy na ikonę ustawień (koło zębate) w prawym górnym rogu, a potem na **Odpowiedź automatyczna**.

2 AUTOMATYCZNA ODPOWIEDŹ Z WYKORZYSTANIEM REGUŁ I SZABLONÓW

Jeśli korzystamy na przykład z konta Gmail podłączonego do Outlooka, konfiguracja automatycznej odpowiedzi jest bardziej skomplikowana i wymaga korzystania z szablonów i reguł.



1 W programie Outlook tworzymy nową wiadomość e-mail.

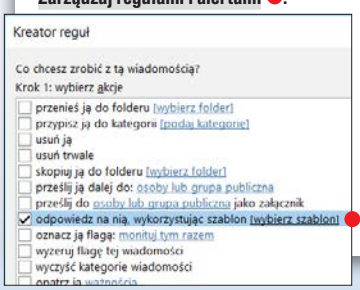


2 Wprowadzamy temat i treść wiadomości dla szablonu dotyczącego naszej nieobecności.

3 Wybieramy opcję **Plik**, a potem polecenie **Zapisz jako**.

4 Nadajemy nazwę szablonowi i z listy rozwijanej **Zapisz jako typ** wybieramy opcję **Szablon Outlook (*.oft)** i klikamy na **Zapisz**.

5 Teraz wykorzystamy ten szablon do utworzenia reguły o nieobecności. Klikamy w głównym oknie programu Outlook na **Plik**, **Zarządzaj regułami i alertami**.



6 Klikamy na **Nowa reguła**, wybieramy **Zastosuj regułę do odbieranych wiadomości** i przechodzimy **Dalej**. Na kolejnym ekranie nie zaznaczamy żadnych warunków i przechodzimy **Dalej**.

7 Potwierdzamy ostrzeżenie, że reguła będzie stosowana do wszystkich wiadomości, klikając na **Tak**.

8 W kolejnym kroku zaznaczamy opcję **Odpowiedz na nią, wykorzystując szablon**, wybieramy, jaki szablon ma być wykorzystany, i klikamy na **Dalej**.

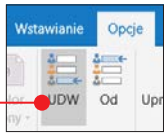
9 Na koniec zaznaczamy opcję **Włącz tę regułę** i klikamy na **Zakończ**.

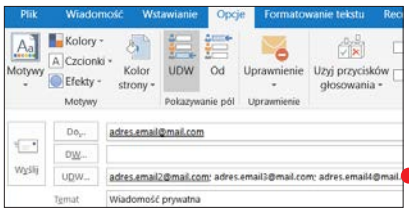
Jeśli potem zachcemy wyłączyć regułę, możemy to zrobić, korzystając z menu z kroku **5**.

3 UKRYWAMY LISTĘ ODBIORCÓW E-MAILA

Jeśli na przykład wysyłamy zapytania ofertowe do wielu firm i nie chcemy, aby odbiorcy wiedzieli, kto jeszcze otrzymał ten sam e-mail, warto korzystać z pola adresowego **UDW** (Ukryte Do Wiadomości), które domyślnie nie jest aktywne w programie Outlook. Adresy wpisane w to pole nie będą widoczne dla odbiorcy (adresy w polu **DW** – Do Wiadomości – są widoczne).

W Outlooku desktopowym przy tworzeniu nowej wiadomości na górnej Wstążce klikamy na **Opcje**, **UDW**. Pojawi się nowe pole na wpisywanie adresów – **UDW**. W **Outlook.com** pole **UDW** zobaczymy, gdy w oknie nowej wiadomości klikniemy na **UDW** w prawym górnym rogu.





4 OUTLOOK.COM PO POLSKU

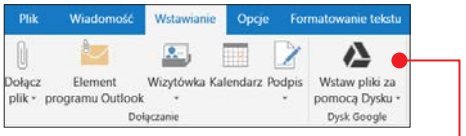
Po uruchomieniu witryny po raz pierwszy może wyświetlić się ona w języku angielskim. Możemy łatwo to zmienić.

Po zalogowaniu się do usługi w przeglądarce przechodzimy do ustawień – klikamy na symbol koła zębatego w prawym górnym rogu, a następnie u dołu na **View all Outlook settings**.

Przechodzimy do kategorii **General**, **Language and time** i w pierwszym polu wybieramy język polski. Po ponownym uruchomieniu witryny wszystkie foldery i opcje powinny wyświetlać się w języku polskim.

Outlook i Outlook.com

5 PODŁĄCZAMY DYSKI CHMUROWE DO OUTLOOKA

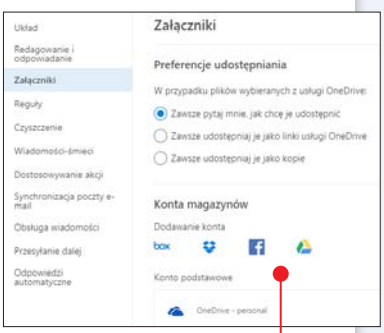


Outlook domyślnie pozwala na dołączanie do wiadomości e-mail plików lokalnych z naszego urządzenia oraz z dysku OneDrive. Możemy jednak dodać kolejne internetowe dyski – Dysk Google, Dropbox itp.

Jeśli chcemy korzystać z dodatkowych dysków w wersji desktopowej Outlooka, musimy pobrać i zainstalować odpowiednie dodatki – **Google Drive for Office** lub **Dropbox for Outlook**.

Jeśli korzystamy z wersji przeglądarkowej – **Outlook.com** – konfiguracja jest prostsza. Po zalogowaniu się do usługi przechodzimy do ustawień – klikamy na symbol koła zębatego w prawym górnym rogu, a następnie u dołu na **Wyświetl wszystkie ustawienia programu Outlook**. Przechodzimy do kategorii **Załączniki** i w sekcji **Konta magazynów** klikamy na ikonę dysku internetowego, który chcemy dodać do naszego konta.

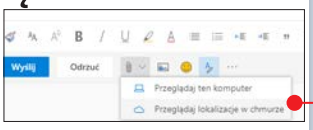
Po poprawnej konfiguracji będziemy mogli dodawać załączniki z wybranego dysku.



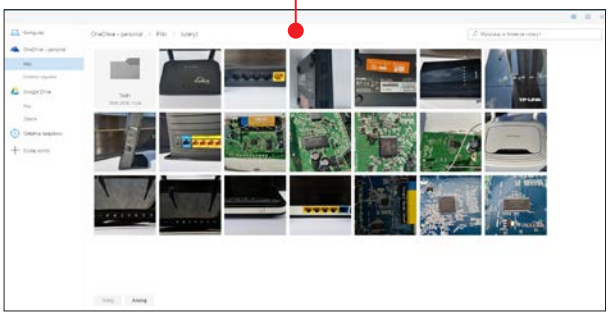
6 WYSYŁAMY BARDZO DUŻE ZAŁĄCZNIKI

Domyślnie Outlook pozwala nam na wysyłanie załączników o maksymalnym rozmiarze dopuszczalnym przez serwer naszej usługi, przeważnie wynosi on 25 MB. Możemy jednak obejść ten limit, wysyłając tylko link do wybranego przez nas pliku znajdującego się na jednym z naszych dysków internetowych połączonych z Outlookiem.

Tworzymy nową wiadomość i dodajemy załącznik, a następnie wybieramy opcję **Przekaż i udostępnij jako link**.

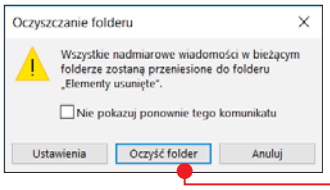


Możemy też po kliknięciu na ikonę załącznika wybrać opcję **Przeglądaj lokalizacje w chmurze**. Wybieramy odpowiedni plik z dysku chmurowego i klikamy na **Dalej** i **Udostępnij jako link**. Załącznik zostanie dodany, wysyłamy wiadomość.

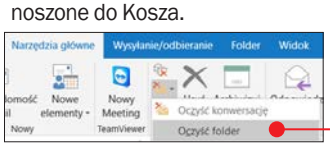


7 SZYBKIE CZYSZCZENIE SKRZYNKI

Po powrocie z urlopu możemy zastać naszą skrzynkę pocztową przepełnioną setkami nowych wiadomości. Warto wtedy skorzystać ze specjalnego narzędzia wbudowanego w Outlook do usuwania duplikatów, powielonych załączników i innych zbędnych wiadomości. Nie musimy się martwić, że jakaś wiadomość zostanie usunięta bezpowrotnie, ponieważ e-maile są przenoszone do Kosza.



W programie Outlook przechodzimy do widoku skrzynki e-mail, a potem na górnej Wstążce klikamy na **Narzędzia główne** i w polu **Usuń** na **Oczyść**, **Oczyść folder**. Potwierdzamy decyzję o przeniesieniu zbędnych wiadomości do Kosza, klikając na **Oczyść folder**. Po chwili pojawi się informacja, ile wiadomości zostało usuniętych. Możemy przejść do ręcznego sprawdzania pozostałych e-maili.



8 APLIKACJA MOBILNA MICROSOFT OUTLOOK

Na smartfonach z Androidem domyślnie jest dostępna poczta Gmail, ale jeśli w pracy korzystamy z Outlooka, możemy go zainstalować także na urządzeniu mobilnym. Wersja mobilna jest darmowa. **kd**

TRIKI DO PROGRAMU *EXCEL*

1 WSKAZÓWEK DO

1 SZYBKIE SUMY

Funkcja **SUMA** jest najczęściej wykorzystywaną funkcją w Excelu. Dlatego doczekała się skrótu klawiaturowego – alt + =.

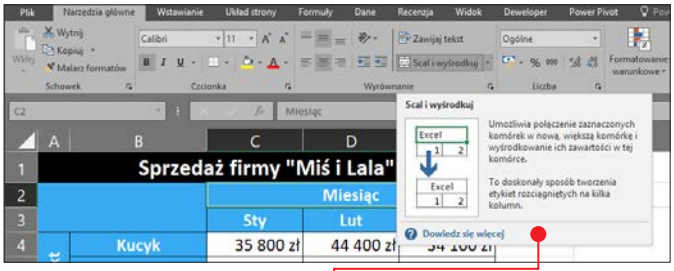
Jeśli naciśniemy ten skrót, to Excel wstawi w zaznaczoną komórkę funkcję **SUMA** i będzie się starał domyślić, po jakim zakresie chcemy sumować. Ponieważ Microsoft wie, że Excelowi nie zawsze udaje się poprawnie zgadnąć zakres sumowania, dlatego zakres w funkcji jest podświetlony i możemy go łatwo zmienić, na przykład zaznaczając inny zakres myszą.

Ale Microsoft nie poprzestał na wstawianiu funkcji **SUMA** tylko do jednej komórki. Skrót klawiaturowy alt + = zadziała także, gdy mamy zaznaczonych kilka komórek, tylko w takiej sytuacji nie będziemy mogli edytować zakresu sumowania przed zatwierdzeniem formuły. Najczęściej jest to przydatne w raportach, gdy potrzebujemy wstawić sumę po kolumnach i wierszach danych. Najwygodniej jest zaznaczyć dane do podsumowania oraz dodatkowo pusty wiersz u dołu i pustą kolumnę na prawo. Teraz, jak naciśniemy skrót alt + =, funkcja **SUMA** wstawi się we wszystkie puste komórki (zaznaczone na zielono).

	A	B	C	D	E
1	Produkt/Miesiąc	Sty	Lut	Mar	
2	Kucyk	35 800 zł	44 400 zł	34 100 zł	114 300 zł
3	Lalka	64 850 zł	55 500 zł	52 350 zł	172 700 zł
4	Miś	51 000 zł	35 500 zł	39 000 zł	125 500 zł
5	Samochód	37 250 zł	18 700 zł	24 150 zł	80 100 zł
6		188 900 zł	154 100 zł	149 600 zł	492 600 zł

Wynik działania skrótu alt + =

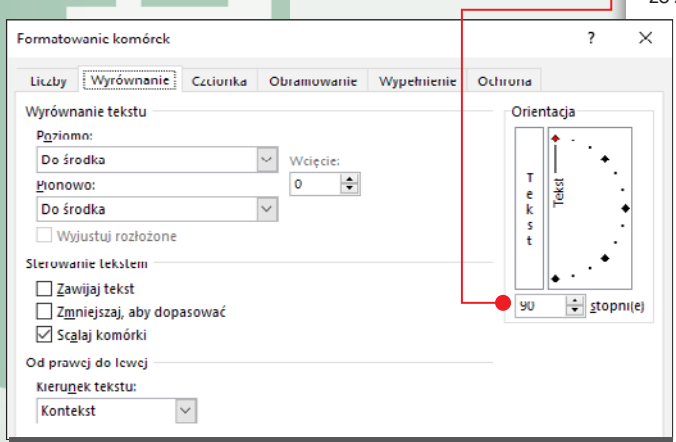
2 SCALANIE KOMÓREK A WYŚRODKOWANIE NA ZAZNACZONYCH KOMÓRKACH W POZIOMIE



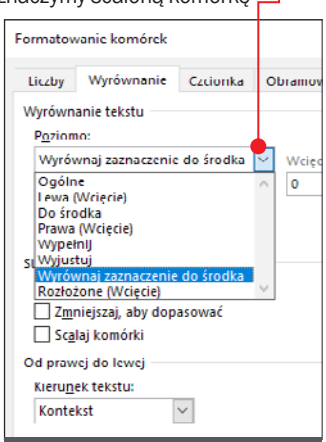
Wiele osób korzysta z opcji **Scal i wyśrodkuj** do wyrównania nagłówków na obszarze wielu kolumn. Na pewno jest to najszybsza opcja, a jeśli chodzi o wyrównanie w pionie – jedyna dostępna.

Uwaga! Przy wyrównaniu w pionie warto jeszcze zmienić orientację tekstu. Zaznaczamy scaloną komórkę, naciskamy ctrl + 1, w oknie **Formatowanie komórek**, które się otworzy, przechodzimy na zakładkę **Wyrównanie** i ustawiamy orientację na 90 stopni.

Scalone komórki sprawiają jednak czasem problemy. Gdy zaznaczamy zakresy komórek przy nich, czasem się zdarza, że zaznaczymy scaloną komórkę i Excel zaznacza obszar szerokości tej scalonej komórki (zaznacza dodatkowe kolumny). Niemożliwe jest też łatwe przenoszenie zakresu scalonych komórek o jedną kolumnę (scalona komórka nachodzi na samą siebie) – Excel na to nie pozwala. Dlatego warto rozważyć alternatywę – **Wyrównaj zaznaczenie do środka**. Żeby skorzystać z tej opcji, wystarczy zaznaczyć komórki, na których chcemy wprowadzić wyrównanie w poziomie (jak przy scalaniu i wyśrodkowaniu komórek), nacisnąć ctrl + 1, przejść do zakładki **Wyrównanie okna formatowania komórek** oraz rozwinąć listę przy wyrównaniu w poziomie i wybrać pozycję **Wyrównaj zaznaczenie do środka**.



Okno formatowania komórek, opcje wyrównania



Opcje wyrównania w poziomie

Scalone komórki C2:E2 oraz A4:A7

Wyrównane na zaznaczeniu A1:E1

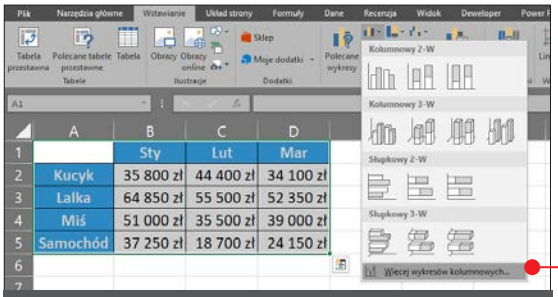
Excel

Excel to ulubieniec wielu użytkowników Office'a, uważany za najważniejszy i najbardziej ceniony program pakietu biurowego Microsoftu. Jest dopracowany i ma bardzo wiele możliwości. ***Poznajmy kilka ciekawych, przydatnych na co dzień trików*** *do Excela*

3 WSTAWIANIE DOMYŚLNEGO WYKRESU

Jeżeli zaznaczymy dane i naciśniemy skrót alt + F1, to wstawimy domyślny wykres na arkuszu z danymi. Jeśli zamiast skrótu klawiaturowego alt + F1 naciśniemy F11, to domyślny wykres wstawi się na nowym osobnym arkuszu. Pozostaje pytanie: Gdzie można zmienić typ domyślnego wykresu?

Od Excela 2013, jeśli na karcie **Wstawianie** rozwiniemy opcje dla wstawiania dowolnego wykresu, zobaczymy na samym dole opcję **Więcej wykresów…**.

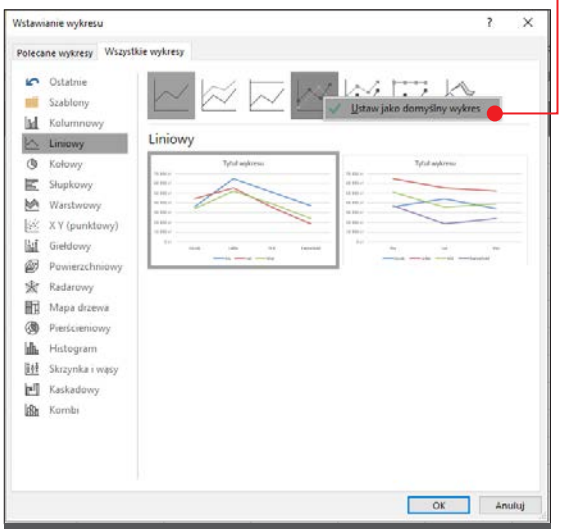


	A	B	C	D
1		Sty	Lut	Mar
2	Kucyk	35 800 zł	44 400 zł	34 100 zł
3	Lalka	64 850 zł	55 500 zł	52 350 zł
4	Miś	51 000 zł	35 500 zł	39 000 zł
5	Samochód	37 250 zł	18 700 zł	24 150 zł
6				

Przechodzenie do wszystkich dostępnych wykresów

W oknie wstawiania wykresów, które się otworzy, wystarczy odszukać wykres, który chcemy, żeby funkcjonował jako wykres domyślny, kliknąć na niego prawym przyciskiem myszy i ustawić jako wykres domyślny.

Od teraz skrót alt + F1 oraz klawisz F11 będą wstawiać wybrany przez nas wykres.



Ustawianie wykresu domyślnego

4 BŁYSKAWICZNE WSTAWIANIE DZISIEJSZEJ DATY I CZASU

Często potrzebujemy wstawić aktualną datę albo godzinę. Robi się to odpowiednio za pomocą skrótów klawiaturowych ctrl + ; (data) oraz ctrl + shift + ; (aktualny czas z dokładnością do minut). Excel wstawia wtedy datę w komórkę (podmieniając wartość, jaka znajdowała się wcześniej w danej komórce) i pozostaje w trybie edycji, czyli możemy dostawić do daty czas (na przykład omawianym skrótem) albo inny komentarz.

Wstawiane wartości są stałe, czyli nie zmienią się tak jak wyniki funkcji **DZIŚ()** albo **TERAZ()**. Wyniki tych funkcji najczęściej przydają się przy formułach do formatowania warunkowego, gdy zależy nam na zaznaczeniu dat przed, po lub równych dzisiejszemu dniowi.

5 SZYBKIE FORMATOWANIE LICZBOWE

Liczby to jeden z typów danych, jakie możemy wstawić w komórki Excela. Bardzo ważne jest, w jaki sposób sformatujemy wartość liczbową, bo od tego zależy, czy będzie reprezentować zwykłą liczbę, godzinę, datę, walutę, procent czy notację naukową. Dlatego warto nauczyć się skrótów klawiaturowych, które ustawiają standardowe style formatowań liczbowych.

	A	B	C	D
1	Formatowanie liczbowe			
2	Przed	Po	Skrót	Formatowanie
3	12345,6	12 345,60	Ctrl + Shift + 1	Formatowanie liczbowe
4	0,625	15:00	Ctrl + Shift + 2	Formatowanie czasu
5	43343	31-sie-18	Ctrl + Shift + 3	Formatowanie daty
6	1234	1 234,00 zł	Ctrl + Shift + 4	Formatowanie walutowe
7	1,23	123%	Ctrl + Shift + 5	Formatowanie procentowe
8	123,456789	1,23E+02	Ctrl + Shift + 6	Formatowanie naukowe
9	2018-08-31	43343	Ctrl + Shift + `	Formatowanie ogólne

6 SZYBKIE FORMATOWANIE TEKSTU

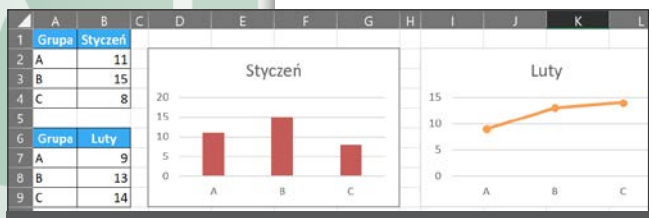
W Excelu często pracujemy nie tylko z liczbami, ale i z tekstem, więc warto się nauczyć skrótów klawiaturowych, które pogrubiają, wstawiają kursywę, podkreślają albo przekreślają, a nawet powtarzają tekst z komórki powyżej.

	A	B	C
1	Szybkie formatowanie tekstu		Skrót
2	**Pogrubienie**	Ctrl + B	Ctrl + 2
3	*Kursywa*	Ctrl + I	Ctrl + 3
4	Podkreślenie	Ctrl + U	Ctrl + 4
5	~~Przekreślenie~~		Ctrl + 5
6	Powtórz tekst		Ctrl + '

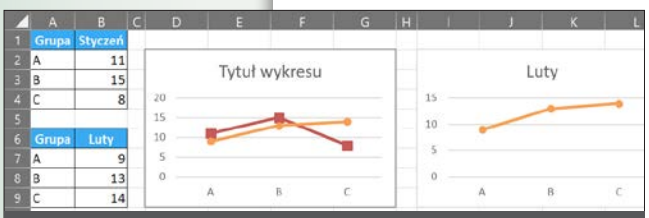
>

7 ŁĄCZENIE WYKRESÓW

Czasami potrzebujemy stworzyć wykresy na podstawie danych z różnych tabel, a nawet z innych arkuszy. W przypadku prostych wykresów możemy zamiast korzystać z polecenia **Zaznacz dane** z karty **Projektowanie Narzędzi wykresów** użyć kopiowania.

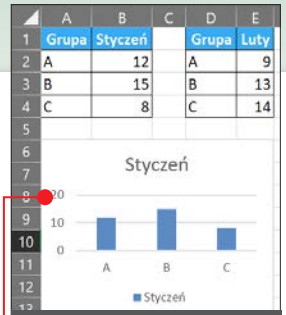


Scalanie wykresów – przed



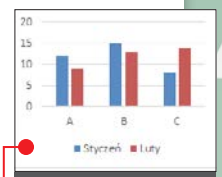
Scalanie wykresów – po

Mamy dwa proste zestawy danych i na podstawie pierwszego z nich stworzyliśmy wykres.



Wykres na podstawie pierwszego zestawu danych

Teraz chcielibyśmy dołożyć drugi zestaw danych do wykresu. Ponieważ zakresy danych są na tej samej wysokości, wystarczy, że zaznaczymy drugi zestaw danych, skopiujemy go (ctrl + C), następnie zaznaczymy wykres i wkleimy do niego (ctrl + V) skopiowane dane – i już mamy wykres, który pokazuje dane z obu zestawów. Jeśli dane nie są w tych samych wierszach, Excel doklei je nie obok (jako nową serię danych) wcześniejszych danych, tylko za nimi (jako istniejącą już serię danych). Wtedy możemy obejść problem, tworząc na podstawie drugiego zestawu danych drugi wykres i to jego skopiować (ctrl + C), a następnie zaznaczyć pierwszy wykres i wkleić (ctrl + V) skopiowany wykres. Dane dokleją się jako nowa seria. Istotne jest również to, że gdy kopiujemy jeden wykres do drugiego wykresu, to skopiuje się również jego typ. Zatem jeśli skopiowaliśmy wykres liniowy i wkleiliśmy go do wykresu kolumnowego, to na wykresie kolumnowym wklejona seria będzie linią.



Wykres po wklejeniu drugiego zestawu danych

8 KOPIOWANIE TYLKO WIDOCZNEGO ZAKRESU KOMÓREK

Kiedy kopiujemy przefiltrowane dane, możemy zobaczyć dużo więcej poziomych linii.

	A	B	C	D
1	Data	Produkt	Sztuk	Sprzedawca
2	2018-06-01	Lalka	2	Mariusz
5	2018-07-08	Robot	3	Mariusz
6	2018-07-11	Miś	2	Ewa
7	2018-07-17	Robot	2	Ewa
10	2018-08-22	Lalka	5	Mariusz
12	2018-08-31	Samochód	4	Ewa

Dzieje się tak, ponieważ Excel automatycznie ogranicza kopiowany zakres tylko do widocznych komórek. Niewidoczne komórki (odfiltrowane) nas nie interesują. Niestety, sytuacja się nie powtarza, gdy ukrywamy wiersze. Excel zaznacza cały zakres i go kopiuje, mimo że zależy nam na skopiowaniu tylko widocznych komórek. Na szczęście istnieje skrót klawiaturowy (alt + ;), który pozwala zaznaczyć tylko widoczne komórki.

	A	C	D
1	Data	Sztuk	Sprzedawca
2	2018-06-01	2	Mariusz
7	2018-07-17	2	Ewa
8	2018-07-18	2	Olga
12	2018-08-31	4	Ewa

Zaznaczanie widocznych komórek może być ciekawą opcją, bo pozwala nam wykluczyć zarówno wiersze, jak i kolumny na przykład z kopiowania czy też ze zmiany formatowania wpisanych w komórki wartości.

9 CIĄGI MIESIĘCY I DNI TYGODNIA (LISTY NIESTANDARDOWE)

W Excelu możemy tworzyć ciągi po listach niestandardowych. Takie wbudowane listy niestandardowe w Excelu to nazwy miesięcy oraz nazwy dni.

Uwaga! Przy dniach pojawiła się zmiana w skrótach w Windows 10, co przeniosło się na ustawienia regionalne, a tym samym na Excela.

Wystarczy, że wpiszemy nazwę miesiąca, jej skrót czy nazwę dnia albo jej skrót i zaczniemy ją przeciągać. Odpowiednio w dół i w prawo listy rosną, a w górę i w lewo listy maleją.

Gdy dojdziemy do końca listy niestandardowej, lista zaczyna się od nowa, czyli przykładowo po grudniu jest znowu styczeń.

Żeby dodać własną listę niestandardową, musimy przejść długą ścieżkę:

Rozpoczynamy od menu **Plik**. Przechodzimy do **Opcji**. Następnie wybieramy zakładkę **Zaawansowane**, którą przewijamy na sam dół i tam odnajdujemy przycisk **Edytuj listy niestandardowe**. Dopiero wtedy otworzy się okno, gdzie będziemy mogli dodać własną listę niestandardową, z której będziemy mogli tworzyć ciągi.

10 NOWE DYNAMICZNE FORMUŁY TABLICOWE

W sierpniu 2018 roku Microsoft pokazał po raz pierwszy nowe funkcje wykorzystujące całkiem nowy sposób działania formuł tablicowych, czyli formuł, które zwracają wiele wyników lub działają na tablicach danych: **https://techcommunity.microsoft.com/t5/Excel-Blog/Preview-of-Dynamic-Arrays-in-Excel/ba-p/252944**

Na razie funkcje, które pokazał Microsoft, są dostępne tylko dla uczestników niejawnego programu testów (listopad 2018), ale już teraz widać ich potęgę. Przyjrzyjmy się wyszukiwaniu unikatowych wartości. Do tej pory trzeba było napisać skomplikowaną formułę:

```
=JEŻELI.BŁĄD(INDEKS(tSprzedaż[Produkt];
PODAJ.POZYCJĘ(0;LICZ.JEŻELI($G$7:G7;
tSprzedaż[Produkt]);0));"")
```

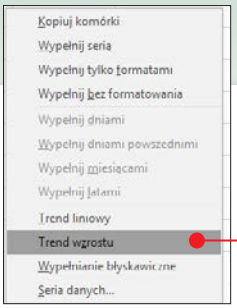
i zastanawiać się, jak daleko ją przeciągnąć, żeby zwróciła wszystkie wyniki, nawet jeśli dane się zmienią.

Po zmianie wystarczy, że użyjemy jednej funkcji:

```
=UNIKATOWE(tSprzedaż[Produkt])
```

a Excel sam ją rozleje odpowiednio daleko, żeby pokazać wszystkie wyniki, nawet jeśli dane ulegną zmianie.

11 CIĄGI LICZB

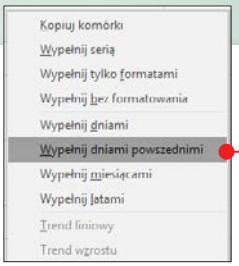


Czasami potrzebujemy w Excelu ciągów liczbowych. W większości sytuacji, jeśli ciągi nie są długie, wystarczy skorzystać z opcji przeciągania danych/komórki. Gdy zaczynamy od pojedynczej liczby i będziemy ją przeciągać w dół, czyli najpierw zaznaczymy komórkę, a następnie złapiemy za jej prawy dolny róg, to Excel będzie nam tę liczbę kopiował. Gdy przy okazji przeciągania będziemy dodatkowo trzymać klawisz ctrl, to ciąg liczbowy w każdym kolejnym wierszu będzie zwiększany o 1. Nie ma znaczenia, czy zaczniemy od liczby dodatniej, ujemnej czy ułamkowej. Wszystko będzie przebiegać tak samo.

A co w sytuacji, gdy chcemy, żeby nasz ciąg zmieniał się o wartość inną niż 1, na przykład rósł o 2? Tym razem potrzebujemy dwóch komórek z danymi. W pierwszą wpisujemy wartość początkową, a w drugą wartość po wzroście, czyli mogą to być przykładowo wartości 1 i 3. Teraz, kiedy zaznaczymy i złapiemy za prawy dolny róg zaznaczenia i zaczniemy przeciągać komórki w dół, to ciąg będzie rósł o 2, czyli wartości w ciągu będą wynosiły 5, 7, 9... Przytrzymanie klawisza ctrl sprawi, że liczby będą się powtarzać, czyli ciąg będzie wyglądał 1, 3, 1, 3, 1... Przy tworzeniu ciągów warto pamiętać, że gdy przeciągamy dane w dół lub w prawo, ciąg rośnie, a gdy przeciągamy w górę lub w lewo, ciąg maleje (na marginesie: rośnięcie i malenie to w zasadzie określenia umowne – możemy zamiast wartości 1 i 3 wpisać w komórki wartość 10 i 8, a wtedy, gdy będziemy przeciągać wartości w dół, ciąg będzie malał o 2, a w górę – będzie rósł).

A co z ciągami geometrycznymi? Co w sytuacji, gdybyśmy chcieli, by każda kolejna liczba w ciągu rosła na przykład dwukrotnie? Musimy zmienić sposób przeciągania – zamiast lewym przyciskiem myszy musimy przeciągać (przynajmniej dwie liczby) prawym przyciskiem myszy. Gdy już przeciągniemy liczby wystarczająco daleko, puszczamy przycisk myszy i z podręcznego menu wybieramy **Trend wzrostu**.

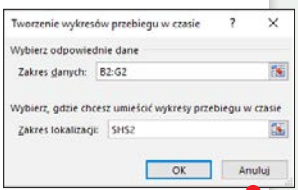
12 CIĄGI DAT



Ponieważ w Excelu daty to z założenia liczby, więc z nich również możemy tworzyć ciągi. Jeśli zaczniemy przeciągać od pojedynczej daty (bez ctrl), to daty będą rosnąć o jeden dzień, a jak przytrzymamy ctrl, to data będzie się powtarzać (odwrotnie niż z liczbami).

Jeśli mamy dwie daty, to uzyskamy ciąg różniący się o ustaloną liczbę dni. Najważniejsze różnice pojawiają się, gdy przeciągamy daty, używając prawego przycisku myszy. Pojawia się dużo więcej możliwości w menu. Możemy wypełniać ciąg tak jak liczbami, czyli dniami, ale możemy też wypełniać go tylko dniami powszednimi, czyli bez sobót i niedziel. Możemy ustawiać daty tak, żeby zmieniał się miesiąc, a dzień miesiąca pozostawał taki sam, możemy nawet wybrać, by daty przeskakiwały o cały rok. Warto wspomnieć o sytuacji, kiedy chcemy mieć ciąg dat konkretnych dni tygodnia, na przykład poniedziałek, wtorek i piątek. Zwykłe przeciąganie nie utworzy nam takiego ciągu. Potrzebujemy formuły, na szczęście prostej – wystarczy, że do pierwszej daty dodamy 7 (dni w tygodniu) **=A1 + 7**. Gdy będziemy przeciągać tę formułę w dół, kolejne wartości będą patrzyły na coraz dawniejsze daty i dodawały do nich cały tydzień – zawsze wyjdą wybrane przez nas dni.

13 WYKRESY PRZEBIEGU W CZASIE



Czasami chcemy stworzyć małe wykresy, które pokazują trend danych. W Excelu idealne są do tego wykresy przebiegu w czasie, które wkleja się w komórkę, czyli są tak duże jak komórka.

Żeby wkleić podobny wykres, zaznaczamy pustą komórkę lub zakres komórek, w których chcemy wstawić miniwykres, a następnie wybieramy odpowiednie polecenie – karta **Wstawianie**, grupa poleceń **Wykresy przebiegu w czasie** – i wybieramy jeden z typów wykresu, na przykład liniowy. Otworzy się okno, w którym musimy zaznaczyć zakres komórek, które mają posłużyć jako dane do wykresu, i zatwierdzamy je przyciskiem **OK**.

Wykresy przebiegu w czasie mają własną kartę **Projektowanie**, gdzie można na przykład zaznaczyć, żeby na wykresie był pokazywany punkt najwyższej i najniższej wartości. Oczywiście można też zmieniać kolorystykę wykresów i punktów. Przykład wstawionych wykresów przebiegu w czasie możemy zobaczyć na rysunku.

Wykres przebiegu w czasie ma rozmiar taki jak komórka, a czasem ciężko dopasować jej rozmiar, by i dane, i wykres wyglądały dobrze. Tu może się przydać informacja, że Excel scalone komórki w większości sytuacji traktuje jak jedną komórkę, więc można stworzyć dużo większy wykres przebiegu w czasie niż pojedyncza komórka.

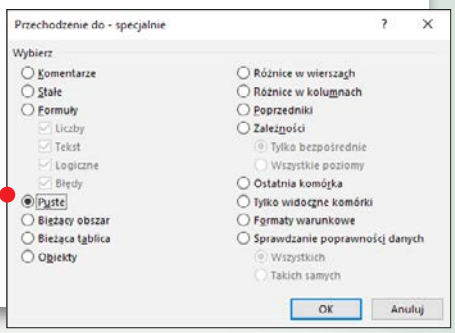
	A	B	C	D	E	F	G	H
1	Produkt	Styczeń	Luty	Marzec	Kwiecień	Maj	Czerwiec	
2	Kucyk	54 051 zł	69 681 zł	90 061 zł	65 388 zł	25 086 zł	54 051 zł	
3	Lalka	40 791 zł	51 617 zł	24 579 zł	26 059 zł	75 009 zł	40 791 zł	
4	Miś	36 550 zł	53 413 zł	79 211 zł	68 353 zł	24 244 zł	36 550 zł	
5	Samochód	75 282 zł	75 242 zł	76 213 zł	26 705 zł	21 730 zł	75 282 zł	

14 WSTAWIANIE WARTOŚCI DO WIELU KOMÓREK NARAZ

Czasami trzeba wstawić tę samą wartość lub formułę do wielu komórek. W Excelu może to być bardzo proste – ze względu na możliwość przeciągania wartości, a także dlatego, że istnieje skrót klawiaturowy, który dokładnie to robi, trzeba tylko zaznaczyć komórki, do których chcemy wpisać konkretną wartość/formułę. Ten skrót to ctrl + enter.

Sprawdza się to jednak tylko w prostych sytuacjach, gdy łatwo możemy zaznaczyć wszystkie komórki, do których chcemy wstawić wartość/funkcję. A co w sytuacji, gdy potrzebujemy wstawić formułę w puste komórki, które znajdują się pomiędzy już wypełnionymi? Oto rozwiązanie.

Najpierw zaznaczamy prostokątny obszar zawierający puste komórki. Następnie na karcie **Narzędzia główne** rozwijamy polecenie **Znajdź i zaznacz** i odszukujemy pozycję **Przejdź do – specjalnie**.



Otworzy się okno, w którym decydujemy, że chcemy zaznaczyć puste komórki. Teraz trzeba tylko uważać, żeby nie usunąć zaznaczenia z komórek i od razu zacząć pisać wartość/formułę, którą chcemy wstawić w puste komórki. Zatwierdzamy ją: ctrl + enter. **ak**

ZOSTAŃ MISTRZEM EXCELA

Autor tych wskazówek – **Adam Kopeć**, znawca i miłośnik Excela – jest autorem książek **Mistrz Excela w 20 dni**, a także **Excel w przykładach** z serii Biblioteczka Komputer Świata. E-wydania obu tytułów można kupić w serwisie **KŚ+ (www.ksplus.pl)**.

TRIKI DO PROGRAMU *WORD*

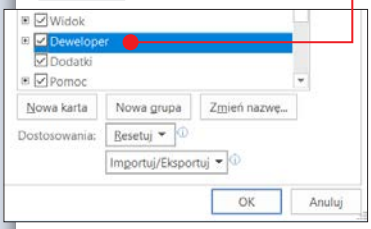
7 WSKAZÓWEK DO

1 „TO DO LIST" W WORDZIE

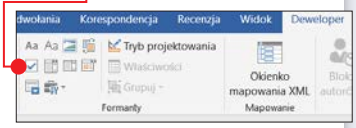
To warto zapamiętać! W Wordzie możemy tworzyć wygodne listy rzeczy do zrobienia czy listy zakupów z polami do „odhaczania" zrealizowanych punktów. Takie listy można przeglądać i edytować na dowolnym urządzeniu, także mobilnym, na którym mamy aplikację obsługującą pliki Worda.

1 Po uruchomieniu pustego dokumentu w programie Word klikamy na **Plik**, a później na **Opcje**.

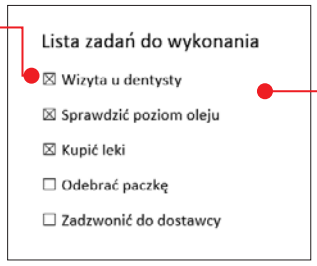
2 Teraz po lewej stronie klikamy na kategorię **Dostosowywanie wstążki**, a następnie po prawej zaznaczamy opcję **Deweloper** i klikamy na **OK**.



3 Na Wstążce klikamy na zakładkę **Deweloper**, a następnie na ikonę **Formant zawartości pola wyboru** w kategorii **Formanty**.



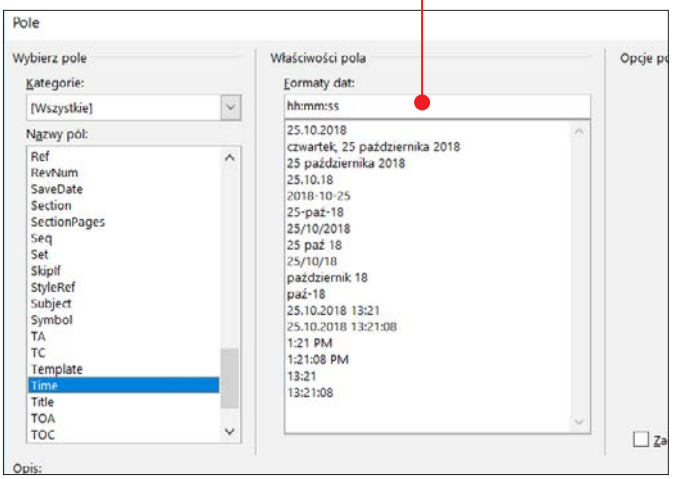
4 Teraz możemy zacząć spisywać rzeczy do zrobienia. Wykonane zadania będziemy zaznaczać, klikając na pola wyboru. Ponowne kliknięcie usuwa zaznaczenie.



2 SZYBKIE DODAWANIE AKTUALNEJ DATY I CZASU

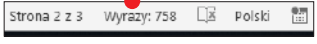
Zdarza się, że tworząc różnego rodzaju dokumenty, musimy dodawać aktualną datę, a czasem nawet godzinę. Zamiast wpisywać je ręcznie, warto korzystać z odpowiednich skrótów klawiaturowych. Po wciśnięciu kombinacji shift+alt+D wstawimy do naszego dokumentu aktualną datę. Natomiast kombinacja shift+alt+T pozwala na dodanie aktualnej godziny.

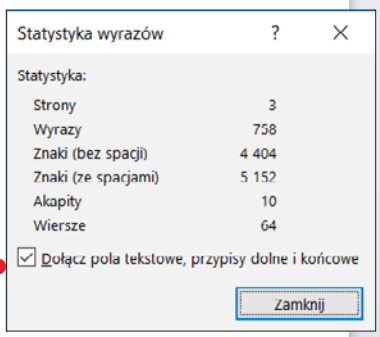
W obydwu przypadkach zostanie użyty format wybrany jako domyślny dla programu Word. Aby zmienić ten format, klikamy prawym przyciskiem myszy na dodane pole tekstowe i wybieramy z listy opcję **Edytuj pole**. Potem wybieramy format, który nam odpowiada.



3 SPRAWDZANIE OBJĘTOŚCI TEKSTU

Jeśli pisząc tekst, musimy zmieścić się w limicie słów lub znaków, warto pamiętać o wbudowanym w program Word narzędziu do automatycznego sprawdzania objętości tekstu. Wystarczy na dolnym pasku po lewej stronie kliknąć na pole **Wyrazy**, a pojawi się okno **Statystyka wyrazów**, gdzie znajdziemy wszystkie potrzebne nam informacje dotyczące objętości tekstu.





4 SZYBKA ZMIANA WIELKOŚCI LITER

Czasem zdarza się, że przez nieuwagę napiszemy kilka wyrazów lub zdań z aktywnym klawiszem caps lock. Aby poprawić taki błąd, zamiast przepisywać tekst od nowa, wystarczy skorzystać z bardzo prostego triku. Zaznaczamy cały tekst, który jest napisany niepoprawnie, i wciskamy kombinację klawiszy shift+F3. Dzięki temu nastąpi zamiana małych liter na duże, dużych na małe.

zDANIE NAPISANE Z WŁĄCZONYM CAPS LOCKIEM.

Zdanie napisane z włączonym caps lockiem.

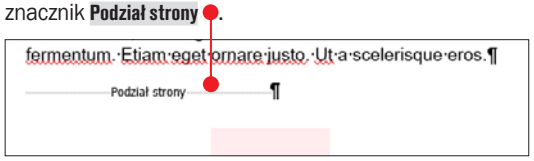
Warto wiedzieć, że w najnowszej wersji programu Word, jeśli zaczniemy pisać nowy wyraz z aktywnym klawiszem caps lock, po wciśnięciu spacji na końcu wyrazu zostanie on automatycznie poprawiony, a przycisk dezaktywowany.

Wo

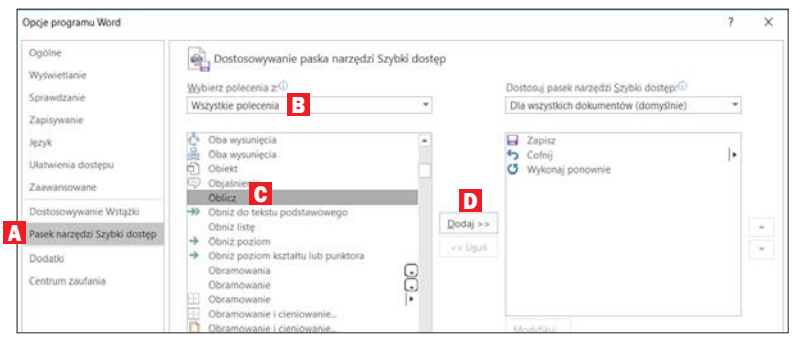
Jeden z najpopularniejszych edytorów tekstowych skrywa w sobie mnóstwo funkcji, o których nawet wieloletni użytkownicy nie mają pojęcia. Warto zapoznać się z tymi ***supertrikami – będą nam ułatwiać pracę*** *każdego dnia*

5 PRZEJŚCIE DO NASTĘPNEJ STRONY

To jeden z najprostszych trików w programie Word. Dzięki niemu możemy natychmiast przejść do edytowania kolejnej nowej strony dokumentu. Wielu użytkowników wielokrotnie wciska w tym celu klawisz enter, jednak nie jest to dobre rozwiązanie, gdyż wtedy przy późniejszej edycji dokumentu i dodaniu nowych fragmentów formatowanie całego dokumentu może być bardzo uciążliwe. Tymczasem żeby przejść do kolejnej strony, wystarczy skorzystać z kombinacji enter+ctrl. Na poprzedniej stronie w trybie podglądu znaczników zobaczymy dodany znacznik **Podział strony**.



6 SPRAWDZAMY POPRAWNOŚĆ OBLICZEŃ



Jeśli tworzymy w Wordzie dokumenty, w których musimy umieszczać obliczenia wraz z wynikami, warto pamiętać, że Word ma wbudowany moduł do sprawdzania poprawności obliczeń.

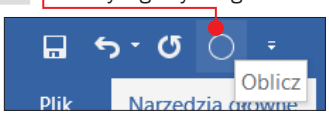
1 Klikamy na **Plik**, **Opcje** i przechodzimy do zakładki **Pasek narzędzi Szybki dostęp** **A**.

2 Wybieramy z listy opcję **Wszystkie polecenia** **B** i odnajdujemy polecenie **Oblicz** **C**. Dodajemy je do paska, klikając na nie i na **Dodaj** **D**, i klikamy na **OK** w celu zachowania zmian.

3 Teraz dodajemy do dokumentu wyrażenie arytmetyczne, które chcemy sprawdzić. Zaznaczamy je w całości, ale

```
(32*43^2) / (23,43-22,43) *15=
```

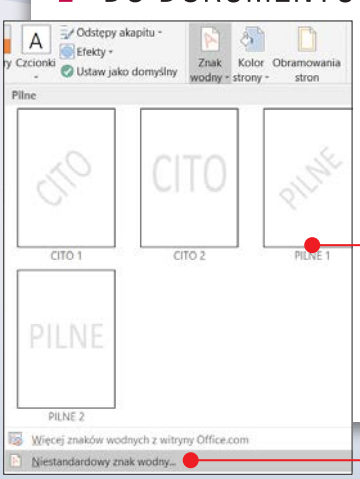
bez znaku =, i klikamy na nową ikonę **Oblicz** w lewym górnym rogu ekranu.



4 W dolnym lewym rogu dokumentu pojawi się wynik obliczeń.

Wynik obliczeń: 887520.

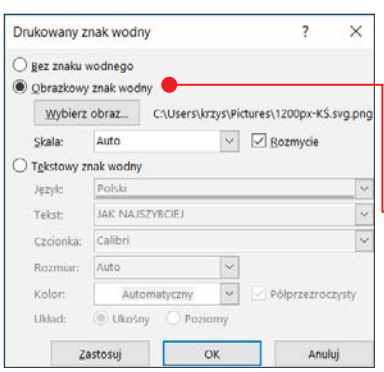
7 DODAJEMY ZNAK WODNY DO DOKUMENTU

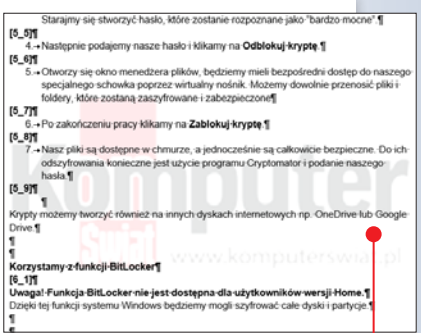


Word pozwala na oznaczanie dokumentów znakiem wodnym, który będzie widoczny także na wydrukach.

1 Aby umieścić znak wodny w dokumencie, na Wstążce klikamy na **Projektowanie** i po prawej stronie na **Znak wodny**. Możemy wybrać jeden ze standardowych znaków.

2 Możemy też dodać własny, na przykład logo firmy itp. – w takim wypadku klikamy na **Niestandardowy znak wodny**. Potem klikamy na **Obrazkowy znak wodny** i na **Wybierz obraz** oraz wskazujemy na dysku potrzebną nam grafikę.




Starajmy się stworzyć hasło, które zostanie rozpoznane jako "bardzo mocne" ¶
[5_5]¶
4.→Następnie podajemy nasze hasło i klikamy na **Odblokuj kryptę**.¶
[5_6]¶
5.→Otworzy się okno menedżera plików, będziemy mieli bezpośredni dostęp do naszego specjalnego schowka poprzez wirtualny nośnik. Możemy dowolnie przenosić pliki i foldery, które zostaną zaszyfrowane i zabezpieczone¶
[5_7]¶
6.→Po zakończeniu pracy klikamy na **Zablokuj kryptę**.¶
[5_8]¶
7.→Nasz pliki są dostępne w chmurze, a jednocześnie są całkowicie bezpieczne. Do ich odszyfrowania konieczne jest użycie programu Cryptomator i podanie naszego hasła.¶
[5_9]¶
¶
Krypty możemy tworzyć również na innych dyskach internetowych np. OneDrive lub Google Drive.¶
¶
¶
Korzystamy z funkcji BitLocker¶
[6_1]¶
Uwaga! Funkcja BitLocker nie jest dostępna dla użytkowników wersji Home.¶
Dzięki tej funkcji systemu Windows będziemy mogli szyfrować całe dyski i partycje.¶
¶

3 Na koniec klikamy na **OK**. Oto efekt.

kd

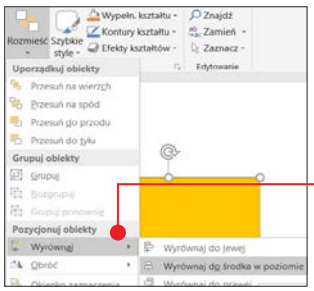
TRIKI DO PROGRAMU *POWERPOINT*

WSKAZÓWEK DO

Program PowerPoint daje nam możliwość tworzenia profesjonalnych prezentacji dzięki wielu dostępnym narzędziom. Nie zawsze jednak łatwo jest zrobić wszystko tak, jak zaplanowaliśmy. Oto ciekawe triki, dzięki którym ***znacznie szybciej stworzymy idealną prezentację***

1 WYRÓWNYWANIE WIELU ELEMENTÓW NA SLAJDZIE

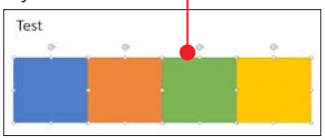
Często po dodaniu kilku różnych elementów do naszego slajdu możemy zauważyć, że nie są one rozmieszczone idealnie. Jeśli zależy nam na wizualnej perfekcji, możemy



bardzo szybko przywrócić symetrię i uporządkowany układ komponentom naszego slajdu.

1 Przytrzymując wciśnięty klawisz shift, klikamy na kolejne elementy, które chcemy uporządkować.

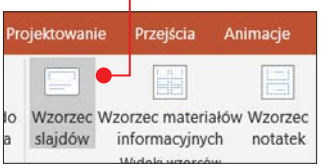
2 Po zaznaczeniu wszystkich klikamy na górnym pasku na **Rozmieść**, **Wyrównaj** i wybieramy potrzebny nam typ rozstawienia. Dzięki temu trikowi zaoszczędzimy dużo czasu.

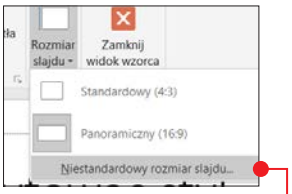


2 ZMIENIAMY DOMYŚLNY ROZMIAR SLAJDU

Nie musimy zawsze trzymać się domyślnych rozmiarów slajdu. Zwłaszcza jeśli zamierzamy prezentować nasze dzieło na monitorze o proporcjach **16:10** lub **21:9**. Ma to kluczowe znaczenie dla odbiorców naszej prezentacji i warto dowiedzieć się, jakie są proporcje ekranu, zanim zaczniemy tworzyć prezentację.

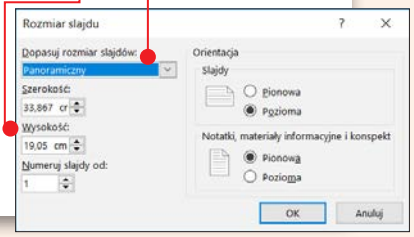
1 Po uruchomieniu programu PowerPoint i przejściu do nowej prezentacji klikamy na **Widok**, **Wzorzec slajdów**





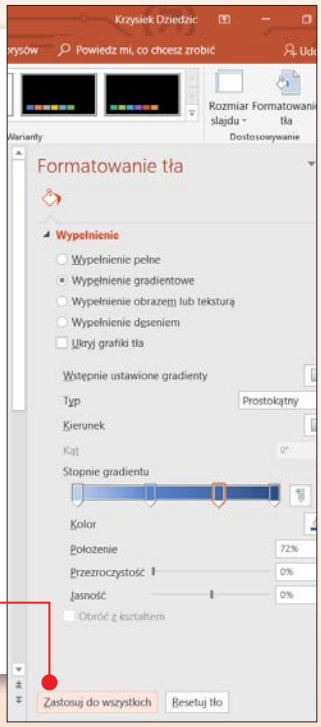
2 Następnie klikamy na **Rozmiar slajdu**, **Niestandardowy rozmiar slajdu**.

3 Wybieramy z listy potrzebny nam format slajdu, a jeśli nie znajdziemy odpowiedniego, możemy wpisać wartości w centymetrach.

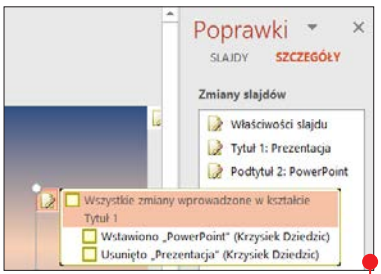


3 TWORZYMY WŁASNY SZABLON

Dostępne w programie PowerPoint szablony nie zawsze idealnie pasują do naszych projektów. Dlatego też warto wiedzieć, jak samemu dodać szablon, który może być podstawą dla naszej prezentacji. Przechodzimy do zakładki **Projektowanie**, a następnie klikamy po prawej stronie na **Formatowanie tła**. Teraz możemy zmieniać wygląd tła naszego slajdu oraz dodawać efekty. Gdy skończymy wprowadzanie modyfikacji, wystarczy kliknąć w prawym dolnym rogu na **Zastosuj do wszystkich**, a wszystkie slajdy naszej prezentacji będą miały taki sam motyw graficzny.



4 ŚLEDZIMY ZMIANY



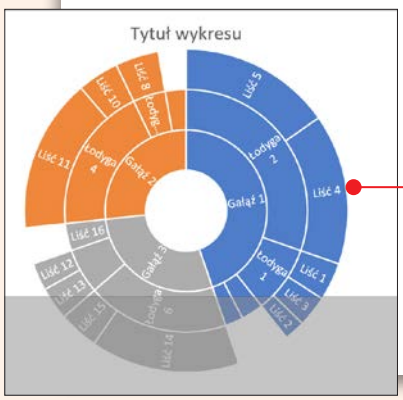
W Wordzie możemy śledzić wszystkie zmiany edycji dokumentu i cofać je, jeśli to konieczne. Niestety, tej funkcji nie oferuje PowerPoint. Na szczęście za pomocą pewnego triku możemy łatwo podejrzeć, co zostało zmienione: wysyłamy dokument PowerPoint do edycji, a nasz oryginał zapisujemy pod inną nazwą. Po uzyskaniu poprawionej wersji otwieramy oryginalny dokument w programie PowerPoint. Na zakładce **Recenzja** klikamy na przycisk **Porównaj**. Następnie wskazujemy poprawioną wersję. Po chwili program PowerPoint wyświetla wszystkie zmiany bezpośrednio w dokumencie. Kliknięciem zatwierdzamy wersję, którą chcemy zachować.

Power t

5 POWIĘKSZANIE SLAJDU W TRAKCIE PREZENTACJI

Bardzo często, gdy tworzymy złożoną prezentację, która zawiera w sobie skomplikowane wykresy, trudno jest pokazać dane w skali odpowiedniej dla odbiorców. Możemy jednak skorzystać z funkcji powiększania slajdów w trakcie ich prezentowania, dzięki czemu będziemy w stanie powiększyć wybrany fragment slajdu i pomóc tym samym widzom w zapoznaniu się ze szczegółami.

Po uruchomieniu prezentacji i przejściu do odpowiedniego slajdu wystarczy, że klikniemy na ikonę lupy w dolnym lewym rogu, a następnie na wybrany fragment prezentacji, który chcemy powiększyć.

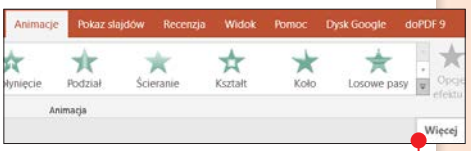


Objęty jasnym polem obszar zostanie odpowiednio powiększony.

Kiedy będziemy chcieli wrócić do normalnego widoku, wystarczy wcisnąć klawisz esc.

6 TWORZYMY WŁASNE ANIMACJE

Warto w naszej prezentacji umieścić animowane elementy, które sprawią, że będzie ona znacznie ciekawsza i przykuje uwagę słuchaczy na dłużej. Jeszcze lepiej będzie, jeśli stworzymy niestandardowe animacje, których nikt wcześniej nie widział.

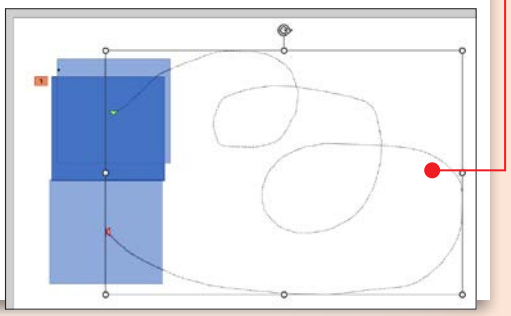


1 Zaznaczamy obiekt, który ma być animowany, i przechodzimy do zakładki **Animacje**. Klikamy na **Więcej**.

2 Następnie na dole strony klikamy na **Ścieżka niestandardowa** w polu **Ścieżki ruchu**.

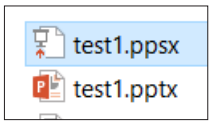
3 Teraz rysujemy na ekranie trajektorię ruchu wybranego obiektu i na koniec wciskamy klawisz enter w celu zatwierdzenia. Animacja zostanie automatycznie uruchomiona, żebyśmy mogli zobaczyć efekt.

4 Możemy jeszcze bardziej dostosować animację do naszych wymagań, na przykład wydłużyć ją lub spowolnić – wystarczy dwukrotnie kliknąć na ścieżkę, a otworzy się okno edycji.

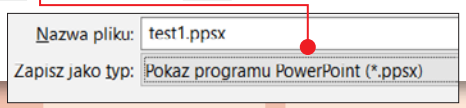


7 NATYCHMIASTOWE URUCHOMIENIE PREZENTACJI

Na ogół, gdy chcemy uruchomić prezentację, klikamy dwukrotnie na plik z rozszerzeniem **PPTX**. Wtedy po chwili uruchamia się program Microsoft PowerPoint w trybie edycji, a my przechodzimy do zakładki **Pokaz slajdów** i klikamy na opcję **Od początku**. Jest to czasochłonne i w dodatku w tym czasie odbiorcy oglądają nasze dzieło w trybie edycji. Znacznie bardziej profesjonalnie wypadniemy, jeśli nasza prezentacja uruchomi się sama po dwukrotnym kliknięciu na plik – oto jak tego dokonać. Cały trik polega na odpowiednim zapisaniu naszej prezentacji, nie jako domyślny plik PowerPoint, ale jako plik **PPSX**, czyli PowerPoint Show – pokaz programu PowerPoint. Klikamy na **Plik**, **Zapisz jako**, wybieramy docelowe miejsce zapisu, a następnie wybieramy typ zapisu – **Pokaz programu PowerPoint** – i klikamy na **Zapisz**.

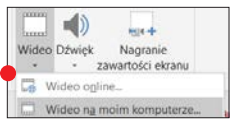


Tak wygląda różnica w wyglądzie ikon pomiędzy pokazem a prezentacją



8 DODAJEMY MULTIMEDIA DO PREZENTACJI

Nasza prezentacja zyska wiele, jeśli dodamy do niej materiały multimedialne, na przykład fragment filmu czy podkład muzyczny. Dodawanie tego typu elementów jest dość proste. Wystarczy po uruchomieniu programu Power Point przejść do wolnego slajdu i kliknąć na górnym pasku na **Wstawianie**. Teraz ze Wstążki wybieramy, jaki element chcemy dodać, w naszym przykładzie jest to plik wideo. Wskazujemy plik, na przykład z naszego dysku, i po dodaniu odpowiednio dopasowujemy jego rozmiar. Możemy również dodać efekt automatycznego uruchamiania filmu przy przejściu do danego slajdu.



kd

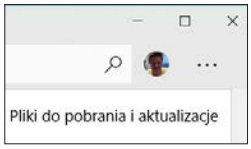
TRIKI DO PROGRAMU *ZDJĘCIA*

1 WSKAZÓWEK DO

*Windows 10 zawiera wydajne narzędzie do fotoedycji – **aplikację Zdjęcia, która ostatnio posługuje się nawet sztuczną inteligencją**. Warto poznać Zdjęcia!*

1 AKTUALIZUJEMY I ZACZYNAMY

Na początek sprawdźmy aktualność aplikacji **Zdjęcia**. Otwieramy program sklepu **Microsoft Store**, klikamy na trzy kropki obok zdjęcia profilowego, na **Pliki do pobrania i aktualizacje** i na **Pobierz aktualizacje**. Teraz, jeśli trzeba, Windows zaktualizuje aplikację **Zdjęcia**. Aby ją uruchomić, w menu Start klikamy na kafelek **Zdjęcia**.



Przy pierwszym uruchomieniu wyświetlenie wszystkich zdjęć trwa dłuższą chwilę.

2 WYBIERAMY ŹRÓDŁA ZDJĘĆ

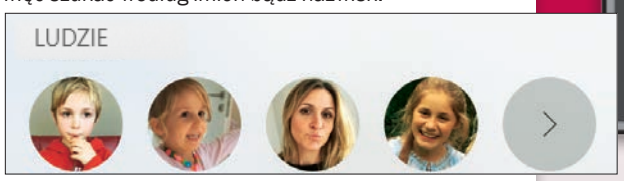
Jeśli aplikacja **Zdjęcia** nie wyświetla wszystkich fotek, trzeba to zmienić. U góry po prawej stronie okna klikamy na trzy kropki i na **Ustawienia**. U góry w sekcji **Źródła** klikamy na **Dodaj folder**, zaznaczamy wybrany folder i klikamy na **Dodaj ten folder do biblioteki „Obrazy”**. Jeśli chcemy zobaczyć nasze zdjęcia zapisane w One Drive, to aktywujemy tę funkcję poniżej, w sekcji **Microsoft OneDrive** (klikamy na przełącznik).

3 SZYBKIE ZNAJDOWANIE ZDJĘĆ I FILMÓW

Szukamy zdjęć z ostatniego urlopu? Oto jak je znaleźć błyskawicznie: kiedy klikniemy u góry okna na **Kolekcje**, pojawi się chronologiczny widok wszystkich zdjęć i filmów. Aby szybko przeskoczyć na przykład do lipca 2017 roku, klikamy na dowolną datę w przeglądzie. Teraz pojawi się lista chronologiczna. Klikamy w niej na wybraną datę, aby zobaczyć zrobione wtedy zdjęcia. Jeśli natomiast szukamy zdjęć w określonym folderze, to po prostu klikamy u góry okna na **Foldery**.

4 SZUKANIE ZDJĘĆ NOWYM WYSZUKIWANIEM POJĘCIOWYM

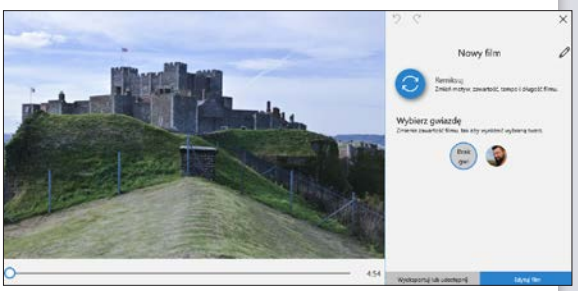
Aplikacja **Zdjęcia** dość dobrze rozpoznaje, co widać na naszych zdjęciach. Ułatwia to wyszukiwanie fotek. Wypróbujmy: w pole wyszukiwania po lewej stronie wpisujemy na przykład **Plaża**. Aplikacja pokaże wszystkie zdjęcia, na których rozpoznała plażę. Podobnie działa wyszukiwanie osób. Po kliknięciu na **Osoby** u góry okna i na puste pole wyszukiwania pojawi się podgląd twarzy, których aplikacja znalazła najwięcej. Klikamy na **Więcej**, aby otworzyć wszystkie znalezione twarze. Po kliknięciu na jedną z twarzy aplikacja **Zdjęcia** pokaże wszystkie fotografie, na których rozpoznała wybraną osobę. Aplikacja (jeszcze) nie oferuje powiązania wyszukiwania osób z naszymi kontaktami, nie możemy więc szukać według imion bądź nazwisk.



Fot. Sasha Lyalina/123rf.com

WINDOWS 10 ZDJĘCIA

5 SZYBKIE TWORZENIE FILMOWYCH POKAZÓW

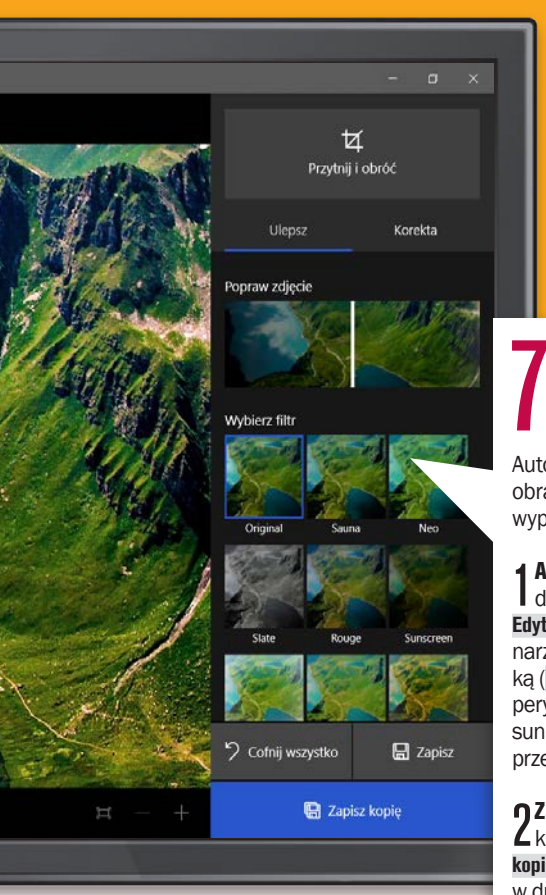


Aplikacja **Zdjęcia** tworzy ciekawie wyglądające wideopokazy zdjęć. W widoku wszystkich folderów albo po kliknięciu na wybrany katalog klikamy u góry okna na **Utwórz** i na **Automatyczny film z muzyką**. Jeśli wcześniej nie wybraliśmy folderu, wskazujemy wybrane fotografie. Nadajemy nazwę projektowi i klikamy na **OK**. Aplikacja **Zdjęcia** automatycznie tworzy wideo ze zdjęć z podkładem dźwiękowym i efektami. Jeżeli program rozpozna twarze, możemy wybrać jedną z nich, by została wyróżniona na pokazie. Jeśli pokaz nam się nie spodoba, mamy dwie możliwości:

- **Zmiksowanie od nowa:** klikamy na przycisk **Remiksuj**. Wtedy aplikacja automatycznie zmontuje zdjęcia jeszcze raz.
- **Edycja ręczna:** klikamy na **Edytuj film**, by dowolnie samodzielnie dostosować do naszych upodobań efekty, muzykę lub narrację i podpisy.

Jeśli jesteśmy zadowoleni z filmu, klikamy na **Wyeksportuj lub udostępnij**. Pokaz zostaje zapisany w jednym z trzech poziomów jakości jako plik MP4 w folderze **Obrazy** na dysku C.

6 NASZE ZDJĘCIA JAKO TŁO PULPITU



Za pomocą aplikacji **Zdjęcia** możemy utworzyć z naszych fotografii tło pulpitu. Klikamy na zdjęcie, aby pojawiło się jako duży obraz w oknie edycji. Klikamy na trzy kropki w prawym górnym rogu okna i wybieramy **Ustaw jako** oraz **Ustaw jak tło**. Aby zdjęcie pojawiało się przy logowaniu po **Ustaw jako**, klikamy na **Ustaw jako ekran blokady**.

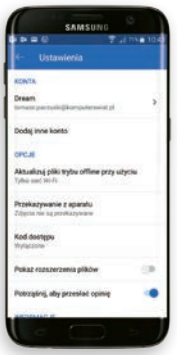
7 ULEPSZANIE ZDJĘĆ JEDNYM KLIKNIĘCIEM

Autokorekta aplikacji **Zdjęcia** błyskawicznie usunie wady obrazu: poprawi kolory, zoptymalizuje kontrast, a nawet wyprostuje zdjęcie. Oto jak to zrobić:

1 Autokorekta: kliknięciem otwieramy zdjęcie do dużego widoku. U góry po prawej stronie klikamy na **Edytuj i utwórz** i na **Edytuj**. Teraz po prawej stronie pojawią się wszystkie dostępne narzędzia. Kiedy pod pozycją **Ulepsz** klikniemy na ikonę z różdżką (**Popraw zdjęcie**), aplikacja zastosuje autokorektę. Poeksperymentujmy z pionowym suwakiem na miniaturze: jeśli przesuniemy go w lewo, autokorekta będzie mniej intensywna, przesunięcie w prawo wzmacnia jej efekty.

2 Zapisanie wyniku: aby zapisać skorygowany obraz, klikamy u dołu po prawej stronie na **Zapisz** albo na **Zapisz kopię**. W pierwszym przypadku oryginał zostanie nadpisany, w drugim – utworzymy kopię ze zmianami (niepoprawiony oryginał zostanie więc zachowany).

KRÓTKIE WSKAZÓWKI DO ZDJĘCIA



8 AUTOMATYCZNE ZAPISYWANIE ZDJĘĆ Z TELEFONU

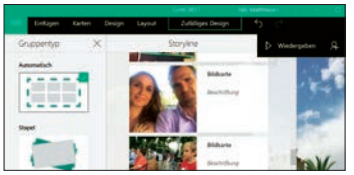
Jeśli chcemy, żeby zdjęcia z telefonu automatycznie pojawiały się w aplikacji **Zdjęcia** na komputerze, to zainstalujmy w telefonie z Androidem bądź z iOS bezpłatną aplikację Microsoftu OneDrive. Po uruchomieniu aplikacji logujemy się na naszym koncie Microsoft i aktywujemy opcję przekazywania z aparatu. Możemy ją skonfigurować, dotykając **Ja**, **Ustawienia**, **Przekazywanie z aparatu**.

9 AUTOMATYCZNE ALBUMY

Aplikacja **Zdjęcia** tworzy automatycznie tak zwane albumy. Nowe albumy znajdziemy po uruchomieniu aplikacji u góry okna. Są one dodawane, jeśli jednego dnia albo w określonym miejscu wykonamy wyjątkowo dużo zdjęć. Albumy zawierają zdjęcia, które według aplikacji są bardziej udane. Aby uzupełnić album, klikamy na **Dodaj zdjęcia**, a żeby samemu stworzyć nowy album, klikamy na **Albumy** i **Utwórz album**. Albumy możemy edytować i udostępniać.

10 DOPIESZCZAMY ALBUMY

Albumy możemy jeszcze bardziej dopracować i na przykład stworzyć z nich interaktywne historie. W tym celu wybieramy album i klikamy na **Udostępnij** w prawym górnym rogu, a potem na **Utwórz swaya**. Po przesłaniu albumu do aplikacji do tworzenia prezentacji Sway możemy eksperymentować z wyglądem, dodawać opisy, animacje i inne efekty.

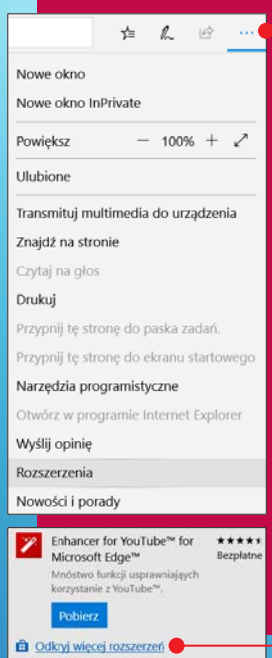


TRIKI DO PROGRAMU *ROZSZERZENIA DO EDGE*

ROZSZERZENIA DO MS EDGE

Edge, przeglądarka Microsoftu wbudowana w Windows 10, jest zawsze pod ręką – łatwo dostępna w systemie. Warto wiedzieć, że teraz obsługuje ona rozszerzenia podobnie jak inne, konkurencyjne przeglądarki. ***Poznajmy najciekawsze dodatki*** *– mogą one znacznie poprawić komfort korzystania z internetu*

JAK ZNALEŹĆ DODATKI DO MS EDGE



Podobnie jak w przypadku przeglądarek Chrome czy też Firefox dodatki do MS Edge znajdziemy w sklepie z rozszerzeniami.

Po uruchomieniu przeglądarki Edge klikamy w górnym prawym rogu na trzy kropki, a następnie na **Rozszerzenia**.

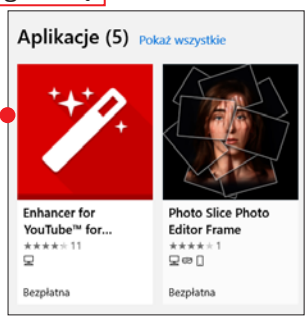
Teraz przechodzimy na sam dół listy i klikamy na **Odkryj więcej rozszerzeń**.

Otworzy się strona sklepu, gdzie będziemy mieli wygodny dostęp do wszystkich rozszerzeń podzielonych na kategorie.

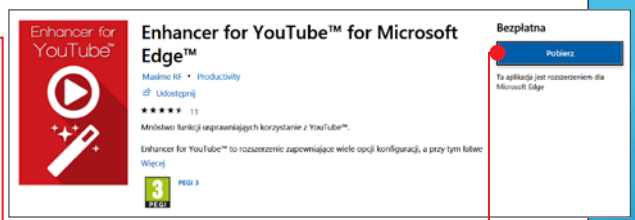
Alternatywnie możemy wejść na stronę: **https://www.microsoft.com/pl-pl/store/collections/edgeextensions**

INSTALUJEMY DODATKI DO MS EDGE

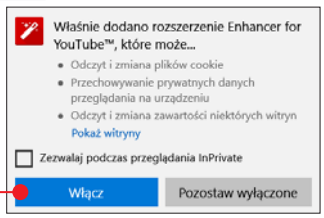
1 Jeśli w sklepie znajdziemy interesujący nas dodatek, wystarczy kliknąć na jego ikonę.



2 Następnie klikamy na przycisk **Pobierz** po prawej stronie ekranu (pod przyciskiem powinna być informacja, że dana aplikacja jest rozszerzeniem dla przeglądarki Edge).



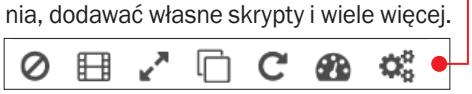
3 Po zainstalowaniu klikamy na **Uruchom**.



4 Wtedy w przeglądarce pojawi się okno z informacją o nowym rozszerzeniu. Musimy jeszcze kliknąć na **Włącz** i już możemy korzystać z nowych funkcji.

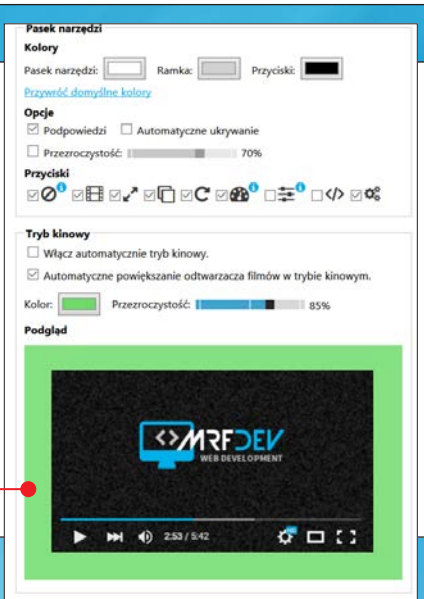
ENHANCER FOR YOUTUBE

Jest to rozszerzenie, które poprawia komfort korzystania z serwisu YouTube. Dzięki niemu będziemy mogli między innymi kontrolować głośność oraz tempo odtwarzania filmów przy użyciu rolki myszy, usuwać adnotacje, automatycznie odtwarzać filmy w zapamiętanej wybranej przez nas rozdzielczości, zapętlać filmy, stosować własne motywy graficzne, używać większego okna odtwarzania, dodawać własne skrypty i wiele więcej.



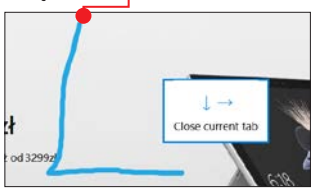
Główne centrum zarządzania tego rozszerzenia znajdziemy na dolnym pasku po uruchomieniu filmu w serwisie YouTube.

Obsługa dodatku jest bardzo intuicyjna i łatwo możemy sami zapoznać się z podstawowymi funkcjami. Zmiana koloru tła wymaga nieco więcej zachodu. Klikamy na **Opcje** na pasku dodatku. Potem przechodzimy do pola **Tryb kinowy** i klikamy na **Kolor**, następnie, korzystając z suwaków, wybieramy idealny kolor tła ekranu odtwarzania. Możemy modyfikować znacznie więcej opcji, a nawet zmienić cały motyw.

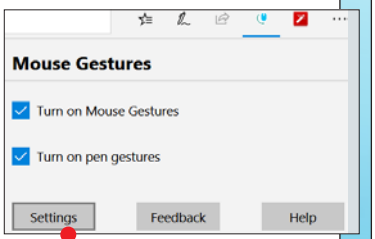


MOUSE GESTURES

To rozszerzenie, które pozwala użytkownikom Edge sterować przeglądarką za pomocą gestów myszy. Podstawowa obsługa polega na wciśnięciu prawego przycisku myszy, a następnie wykonywaniu ruchów myszą. Na przykład przesunięcie w prawo powoduje zamknięcie aktualnie otwartej karty – gesty są widoczne na ekranie naszego urządzenia.



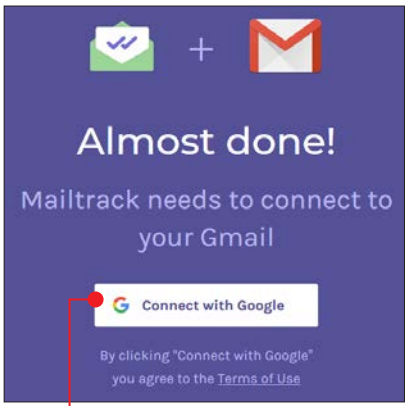
Możemy zmienić przypisaną do danego gestu akcję i sprawdzić, z jakich gestów możemy korzystać. Wystarczy na górnym pasku przeglądarki kliknąć na ikonę rozszerzenia i na **Settings**.



Gestów jest dużo. Korzystanie z nich znacznie przyspiesza pracę z przeglądarką.

MAILTRACK FOR GMAIL AND INBOX

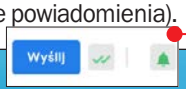
Jest to świetny dodatek, który pomoże nam zorientować się, czy nasza wiadomość e-mail dotarła do adresata, a nawet, kiedy ją przeczytał. To rozszerzenie działa wyłącznie w skrzynkach Gmail oraz Inbox, ale z Gmaila na pewno korzysta wielu z nas.



1 Po instalacji dodatku klikamy na **Connect with Google**.

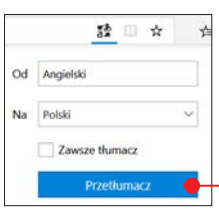
2 Następnie po zalogowaniu się danymi naszego konta Google klikamy na **Sign Up Free**, a następnie na **Go to Gmail**.

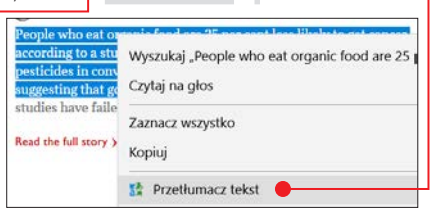
3 Teraz możemy wysyłać wiadomości e-mail i w głównym widoku skrzynki e-mail monitorować ich statusy (jeden ptaszek – dostarczone, dwa ptaszki – dostarczone i odczytane, dzwonek – włączone powiadomienia).



MICROSOFT TRANSLATOR

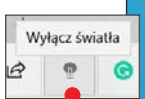
Bardzo przydatne rozszerzenie, które umożliwia szybkie tłumaczenie całych stron i zaznaczonego tekstu w ponad 60 językach. Podczas wyświetlania obcojęzycznych stron wystarczy na pasku adresowym kliknąć na ikonę dodatku Microsoft Translator, a następnie na **Przetłumacz**. Potem warto upewnić się, czy język tłumaczenia został poprawnie wykryty. Możemy również zaznaczać wybrane fragmenty tekstu, a następnie kliknąć prawym przyciskiem myszy i wybrać opcję **Przetłumacz tekst**.

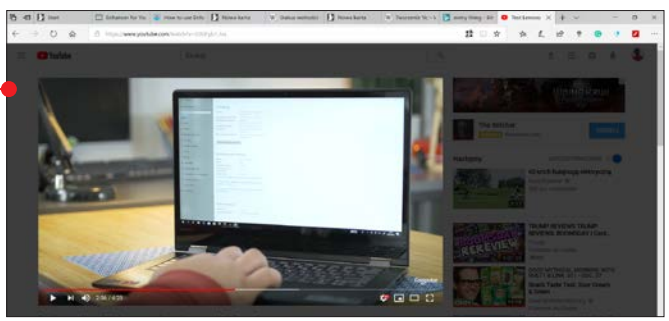




TURN OFF THE LIGHTS

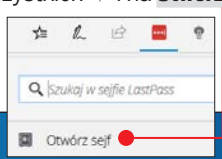
Jest to rozszerzenie, które pozwala na komfortowe oglądanie multimediów w przeglądarce – wygasza tło oglądanego filmu, by nie męczyć oczu. Dodatek ten automatycznie wykrywa wideo. Aby zgasić świat ło na stronie, wystarczy kliknąć na jego ikonę na pasku adresowym. Po ponownym kliknięciu na ikonę zaciemnienie zostanie cofnięte.

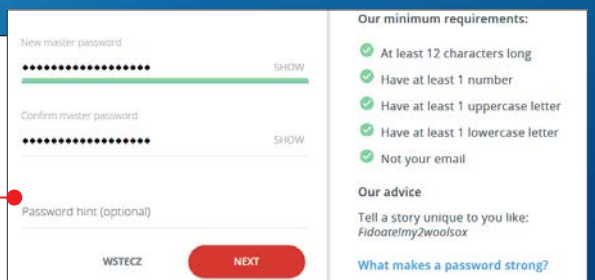




LASTPASS

To rozszerzenie pomoże nam zapanować nad wszystkimi hasłami. Do korzystania z dodatku konieczne jest założenie darmowego konta chronionego jednym hasłem, które będzie nam dawało dostęp do wszystkich innych naszych haseł na każdym urządzeniu z zainstalowanym rozszerzeniem LastPass. Jest to bardzo wygodne rozwiązanie dla zapominalskich. Po założeniu konta możemy zacząć korzystać ze skrytki na hasła – klikamy na ikonę dodatku i na **Otwórz sejf**. Następnie klikamy w prawym dolnym rogu na **Dodaj witrynę** i uzupełniamy formularz poprawnymi danymi, które zapisujemy, klikając na **Zapisz**. Możemy w ten sposób dodawać również foldery i inne elementy, które ułatwią nam zarządzanie wszystkimi hasłami. **kd**





TRIKI
DO PROGRAMÓW
PRZEGLĄDARKI

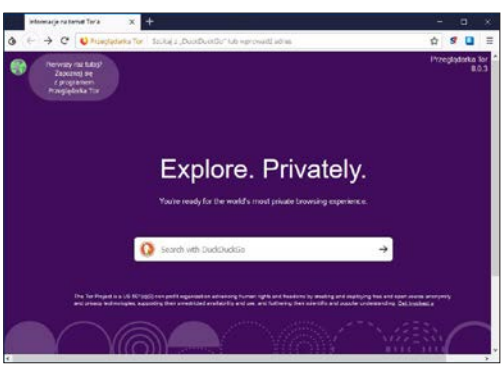
BEZPIECZNE PRZEGLĄDARKI

Najpopularniejsze przeglądarki, jak Chrome, Firefox, Edge, są wygodne i dopracowane. Warto jednak poznać alternatywy, które mają jedną ważną przewagę: ***zapewniają większą prywatność***

Podczas przeglądania sieci mamy dostęp do niezliczonych informacji, sami – często nieświadomie – wiele informacji wysyłamy. Wśród nich są nasze preferencje wyszukiwania, historia pobieranych plików, a nawet dokładna lokalizacja. Żeby zadbać o prywatność, warto korzystać z bezpiecznej przeglądarki. Oto kilka programów, które umożliwią nam przeglądanie internetu bez obaw o to, że nasze dane trafią w niepowołane ręce. **bs**

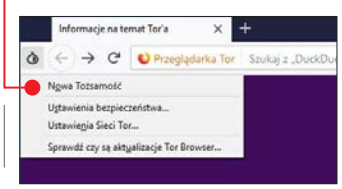
TOR BROWSER

Tor Browser (DVD-KOD: **059/060**, 32-/64-bit) to darmowy pakiet, który gwarantuje anonimowość przeglądania internetu. Działa on na bazie Firefoxa, dodając do niego funkcjonalność przekierowywania połączeń pomiędzy komputerami przekaźnikami na całym świecie. Sprawia to, że wyśledzenie naszego komputera, a co za tym idzie także i naszej tożsamości, jest praktycznie niemożliwe.



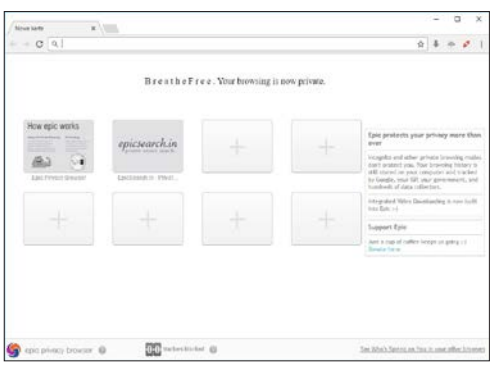
Po instalacji pakietu zmodyfikowaną wersję Firefoxa włączymy za pomocą ikony Start Tor Browser. Po uruchomieniu przeglądarki nastąpi krótkie łączenie i trafimy na stronę startową, z której możemy już swobodnie i bezpiecznie przeglądać internet.

Z powodu konieczności przekierowywania sygnału pomiędzy przekaźnikami na całym świecie korzystanie z Tor Browsera w widoczny sposób spowalnia ładowanie się zawartości stron internetowych. W przypadku gdy czas ten jest wyjątkowo długi, można zmienić łańcuch połączeń, klikając na ikonę w lewym górnym rogu okna, a następnie wybierając opcję **Nowa tożsamość**. Spowoduje to połączenie się z siecią za pośrednictwem nowego zestawu przekaźników, co może przyspieszyć działanie.



EPIC PRIVACY BROWSER

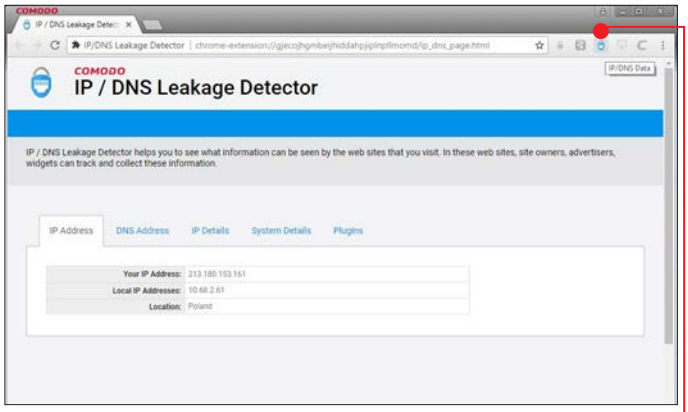
Epic Privacy Browser (DVD-KOD: **015**) to jedna z najbardziej złożonych przeglądarek, która dba o bezpieczeństwo danych użytkownika na bardzo wielu polach. Epic Privacy opiera się na kodzie Chromium, rozszerzając go jednak o dodatkowe funkcjonalności.



Działanie Epic Privacy Browser oparte jest na kilku filarach. Pierwszym z nich jest wyłączenie wszelkich funkcji, umożliwiających śledzenie naszych preferencji, w tym autouzupełniania, korekty treści, tłumaczeń czy zapisywania logów o błędach. Przeglądarka blokuje także reklamy, ciasteczka, skrypty śledzące, koparki kryptowalut zaszyte na stronach i widżety z nieznanych źródeł. Po zakończeniu pracy z przeglądarką usuwane są z niej wszelkie informacje, w tym historia, pamięć podręczna, informacje o logowaniach i wszelkie inne dane, które umożliwiają prześledzenie naszych preferencji. To również jedna z niewielu przeglądarek, która chroni naszą prywatność przed dostawcą usług internetowych.

Ważną funkcjonalnością Epic Privacy jest możliwość uruchomienia szyfrowanego połączenia proxy za pomocą jednego przycisku. Aktywujemy go ikoną w prawym górnym rogu przeglądarki. Po aktywacji możemy również wybrać kraj, z którego serwera chcemy korzystać – nasze IP będzie od tej chwili widoczne tak, jakbyśmy znajdowali się na jego terytorium.

COMODO DRAGON



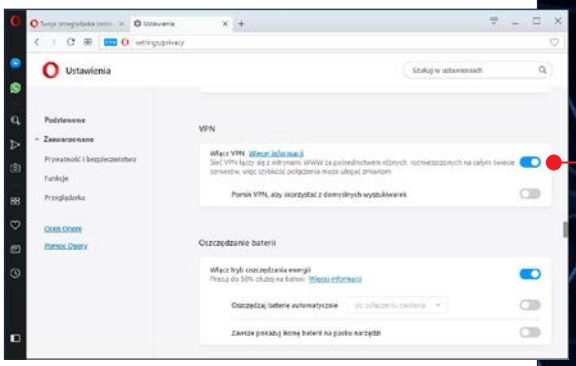
Przeglądarka **Comodo Dragon** (DVD-KOD: **010**) oparta jest na kodzie Chromium, ale zmodyfikowanym przez firmę Comodo, znaną z produkcji systemów bezpieczeństwa. Jej stworzeniu przyświecały dwa cele: poprawa szybkości i prywatności względem najpopularniejszych przeglądarek.

Za szybkość działania Comodo Dragon odpowiada znany z Chromium silnik renderujący WebKit, a sam program jest maksymalnie odciążony ze zbędnych elementów. Usunięto między innymi pakiet skryptów, których Google używa do śledzenia działań użytkowników. Niewątpliwą zaletą Comodo Dragon jest stabilność działania – przeglądarka zużywa niewiele pamięci RAM, a zawieszenie się jednej karty nie zawiesza działania całego programu.

Comodo Dragon uczula nas na niebezpieczeństwa, które czyhają w trakcie przeglądania internetu – wyświetla rozszerzone informacje o zabezpieczeniach SSL. Blokuje także ciasteczka i skrypty szpiegujące oraz zabezpiecza informacje o pobranych przez nas plikach.

Dodatkową, ciekawą funkcją Comodo Dragon jest pokazywanie, które z informacji o nas są widoczne dla stron, jakie odwiedzamy. Aby je zobaczyć, należy kliknąć na ikonę w prawym górnym rogu okna programu.

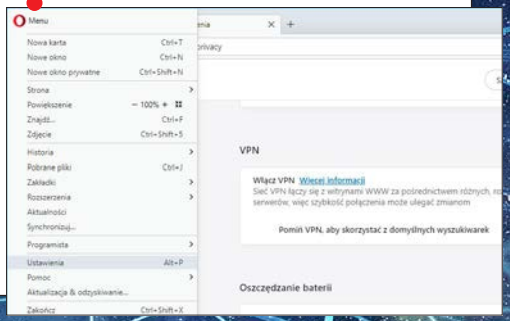
OPERA



Opera (DVD-KOD: **041**) to jedyna przeglądarka, która oferuje możliwość zadbania o bezpieczeństwo za pomocą darmowej i nieograniczonej sieci VPN, dostępnej bez konieczności instalowania dodatkowych rozszerzeń, uiszczania opłat czy rejestrowania się na zewnętrznych stronach.

Sieć VPN zastępuje adres IP użytkownika adresem wirtualnym, utrudniając w ten sposób śledzenie naszej prawdziwej lokalizacji, a co za tym idzie – także tożsamości. Tego typu rozwiązanie jest bardzo przydatne, jeżeli korzystamy z internetu w miejscach publicznych, za pośrednictwem otwartych hotspotów Wi-Fi. VPN Opery chroni naszą aktywność przed atakami ze strony innych użytkowników tej samej sieci publicznej.

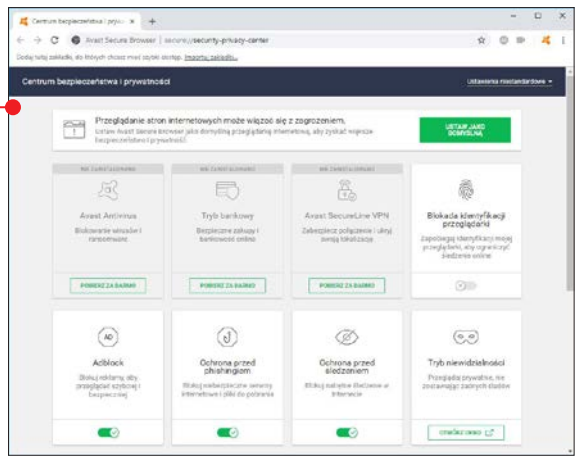
Aby uruchomić sieć VPN w Operze, należy rozwinąć menu w lewym górnym rogu okna przeglądarki, a następnie wybrać opcję **Ustawienia**. Z rozwijalnego menu **Zaawansowane** należy wybrać opcję **Prywatność i bezpieczeństwo**, a następnie kliknąć na **Włącz VPN**. Korzystanie z funkcji VPN jest cały czas sygnalizowane niebieską ikoną na pasku adresu.



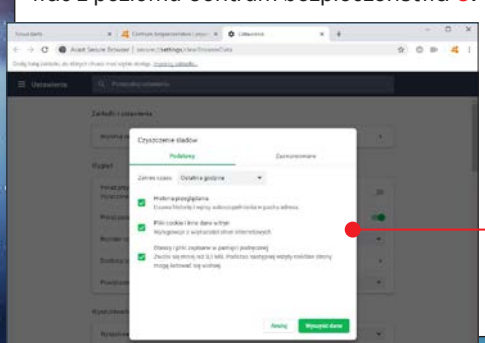
AVAST SECURE BROWSER

Avast Secure Browser (DVD-KOD: **004**) to kolejna przeglądarka, której bazą jest kod Chromium. Za jej stworzenie odpowiadają twórcy popularnego darmowego systemu bezpieczeństwa Avast Free Antyvirus.

Przeglądarka Avasta oferuje wiele modułów bezpieczeństwa, które możemy aktywować z poziomu Centrum bezpieczeństwa.



Dostęp do niego uzyskamy, klikając na ikonę w prawym górnym rogu okna przeglądarki. W Centrum bezpieczeństwa możemy wybrać, które z funkcji bezpieczeństwa chcemy mieć aktywowane. Wśród nich znajdziemy preinstalowaną blokadę reklam, ochronę przed phishingiem (wyłudzaniem haseł), ochronę przed śledzeniem, blokadę rozszerzeń, szyfrowanie HTTPS i ochronę przed obiektami flash. Ponadto możemy włączyć blokadę identyfikacji przeglądarki, co zmniejsza ilość danych, jaką mogą o nas uzyskać strony internetowe. Za pomocą funkcji **Czyszczenie śladów** możemy także usunąć wszystkie dotychczasowe ślady naszej aktywności w sieci.



Część opcji, w tym tryb bankowy (zabezpieczający transakcje internetowe) i VPN, jest domyślnie niedostępna i oznaczona szarym kolorem. Możemy uzyskać do nich dostęp, klikając na przycisk **Pobierz za darmo** pod wybraną funkcją.

Fot. Sergey Nivens/123rf.com

TRIKI
DO PROGRAMÓW
SZYFROWANIE

ZABEZPIECZANIE

*Oto kompletny poradnik, jak zadbać o bezpieczeństwo danych na komputerze. Dzięki **szyfrowaniu zasobów** nikt oprócz nas nie będzie mógł uzyskać do nich dostępu. Przeczytajmy, jak na różne sposoby zabezpieczać różnego rodzaju dane*

Skuteczne zabezpieczenie naszych plików może być bardzo dobrą polisą na wypadek kradzieży czy zgubienia laptopa, dysku zewnętrznego czy nawet pendrive'a. Samo hasło do systemu nie jest praktycznie żadną ochroną, jeśli ktoś będzie chciał dostać się do naszych danych. Dlatego warto zadbać o szyfrowanie. Po odpowiedniej konfiguracji dostęp do naszych danych bez znajomości metody autoryzacji będzie praktycznie niemożliwy. W zależności od tego, jaki sprzęt i jakie dane chcemy zabezpieczyć, możemy skorzystać z różnych metod.

W tym poradniku przeczytamy, jak korzystać ze specjalistycznych narzędzi do szyfrowania dysków, partycji, nośników USB, a nawet przestrzeni w chmurze. Przeanalizujemy też możliwość szyfrowania z wykorzystaniem wbudowanego w Windows narzędzia BitLocker. **kd**

SZYFROWANIE CAŁEGO DYSKU CZY WYBRANEJ PRZESTRZENI

Wielu użytkowników staje przed tym dylematem. Ze względu na bezpieczeństwo lepiej jest korzystać z szyfrowania całego dysku. Ze względu na wydajność i sprawność pracy często lepszym wyjściem jest jednak zaszyfrowanie wybranej przestrzeni dysku – utworzenie sejfu, tak zwanej krypty, w której przechowywać będziemy wybrane pliki i dokumenty. Obecnie coraz więcej osób korzysta w swoich komputerach z szybkich i wydajnych dysków SSD, a w ich przypadku zaszyfrowanie całego nośnika nie wpływa znacząco na obniżenie wydajności, a poprawia bezpieczeństwo danych. Jeśli jednak korzystamy ze starego nośnika HDD, bardziej optymalnym rozwiązaniem będzie utworzenie zaszyfrowanego magazynu na części partycji.

SZYFRUJEMY Z VERACRYPT

Jeśli interesuje nas maksymalne bezpieczeństwo naszych nośników danych, warto skorzystać z pomocy programu VeraCrypt. Możemy zaszyfrować cały dysk, wybraną partycję, a nawet wybrane nośniki USB. Często przenosimy poufne dane na pendrive'ach, a są one najbardziej podatne na kradzież lub zgubienie. Jeśli będą odpowiednio przez nas zabezpieczone, osoby trzecie nie uzyskają dostępu do naszych danych. Oczywiście zaszyfrowanie całego dysku w większości przypadków oznacza spadek wydajności, nie jest on drastyczny, jednak zdecydowanie odczuwalny. Program oferuje nam wiele różnych algorytmów szyfrujących i bardzo ciekawą opcję szyfrowania kaskadowego, które pozwala na wykorzystanie kilku algorytmów do szyfrowania danego nośnika.

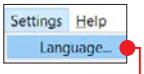
SZYFROWANIE Z MICROSOFT BITLOCKER CZY Z VERACRYPT

Funkcja szyfrowania dysku BitLocker dostępna jest tylko w wersji Pro, Enterprise lub Education systemu Windows. Wykorzystuje ona moduł TPM, jeżeli nasze urządzenie taki ma, a jeśli nie – będziemy musieli skorzystać z dodatkowego nośnika, takiego jak pendrive. Zabezpieczony dysk będzie całkowicie bezpieczny w przypadku zwykłego ataku. Prośba o weryfikację pojawia się, zanim załadowany zostanie system. Warto jednak rozważyć korzystanie z programu VeraCrypt, który oferuje bardzo podobne rozwiązanie, uważane nawet za bezpieczniejsze. Największa różnica między tymi dwoma metodami polega na tym, że BitLocker to funkcja systemu i nie wiadomo, czy Microsoft nie ma specjalnego algorytmu, który może odblokować każdy zaszyfrowany zasób – oczywiście są to tylko spekulacje. W przypadku VeraCrypt mamy do czynienia z otwartym oprogramowaniem, które przeszło wiele audytów bezpieczeństwa i wydaje się nie mieć wad w kodzie. Dodatkowo VeraCrypt pozwala nam na szyfrowanie nośników USB oraz wybranej przestrzeni dysku, a nie całej jego powierzchni.

	BitLocker	VeraCrypt
Dostępność	Windows Pro, Enterprise, Education	Dla każdego
Opcje szyfrowania	Cała partycja	Partycja lub jej część
Kompatybilność przy przenoszeniu nośników	Przy zabezpieczeniu TPM nie możemy przenosić dysku między komputerami	Działa na każdym komputerze z zainstalowanym programem VeraCrypt

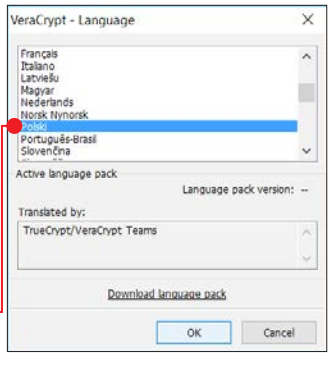
ZMIANA JĘZYKA

Zanim zaczniemy korzystać z programu, warto zmienić domyślny język z angielskiego na polski.



1 Po uruchomieniu programu klikamy na **Settings**, **Language**.

2 Z listy wybieramy **Polski** i klikamy na **OK**.

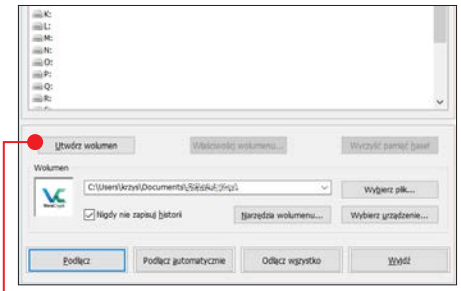


DANYCH – SZYFROWANIE

TWORZYMY ZASZYFROWANY WOLUMEN

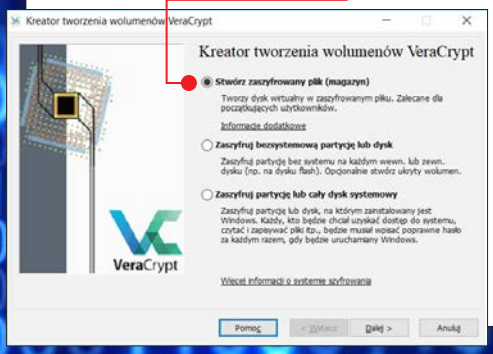
Zaszyfrowany wolumen to zaszyfrowany magazyn wydzielony z naszego dysku.

1 Po zainstalowaniu uruchamiamy program VeraCrypt.

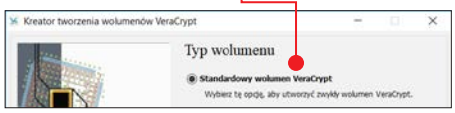


2 Teraz musimy kliknąć na **Utwórz wolumen**.

3 Pozostawiamy wybraną domyślnie opcję **Stwórz zaszyfrowany plik** i klikamy na **Dalej**.



4 Następnie wybieramy opcję **Standardowy wolumen VeraCrypt** i klikamy na **Dalej**.



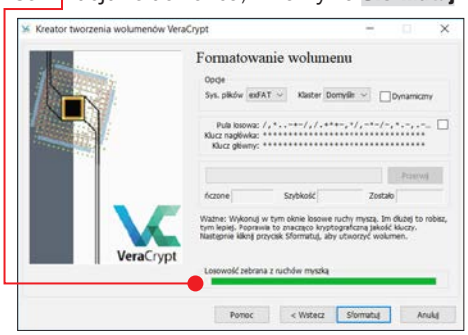
5 Klikamy na **Wybierz plik**, musimy podać nazwę naszego wolumenu i jego lokalizację. **Uwaga!** Nie wybierajmy istniejącego pliku, gdyż zostanie on skasowany – pliki do zaszyfrowania przenosimy do wolumenu dopiero po jego utworzeniu.

6 Pozostawiamy ustawienia algorytmów szyfrujących i mieszania bez zmian i klikamy na **Dalej**.

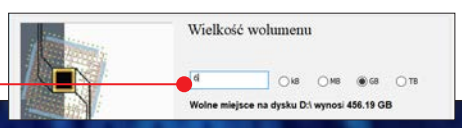
7 Podajemy rozmiar wolumenu, zwróćmy uwagę na jednostki, w których podajemy dane. Po wpisaniu wartości klikamy na **Dalej**.

8 Następnie podajemy hasło, które będzie chroniło nasz wolumen. Rekomendowane jest hasło o długości przynajmniej 20 znaków. Najlepiej jeśli będzie zawierało również przynajmniej jedną dużą literę, cyfrę i znak specjalny.

9 W kolejnych krokach musimy określić, czy będziemy przechowywać pliki większe niż 4 GB. Jeśli tak, wybieramy system plików **exFAT** lub **NTFS**. Musimy również wykonywać losowe ruchy myszą w celu poprawy kryptograficznej jakości generowanych kluczy. Dopiero gdy pasek dojdzie do końca, klikamy na **Sformatuj**.



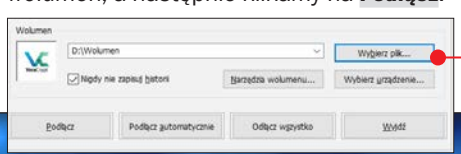
10 Po utworzeniu wolumenu klikamy na **Zakończ**.

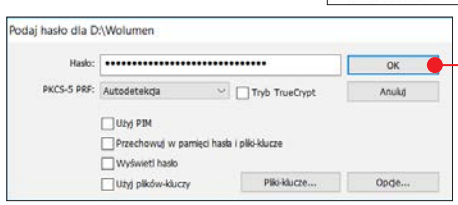


MONTUJEMY WOLUMEN

Zanim zaczniemy korzystać z naszego sejfu, musimy go zamontować.

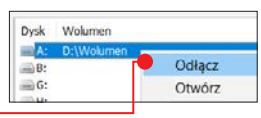
1 W głównym oknie programu VeraCrypt klikamy na **Wybierz plik**. Wybieramy nasz wolumen, a następnie klikamy na **Podłącz**.





2 Podajemy hasło i klikamy na przycisk **OK**.

3 Po udanej weryfikacji nasz zasób zostanie dodany jako **nowy dysk** i będziemy mogli korzystać z niego tak jak ze zwykłego dysku – kopiując, zapisując pliki itp. Po zakończeniu pracy w programie VeraCrypt klikamy na wolumen prawym przyciskiem myszy, i z menu wybieramy opcję **Odłącz**.

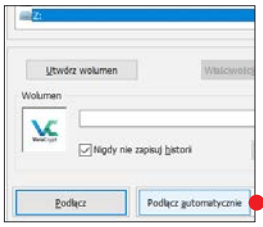


Fot. Nikita Bonin/123rf.com

UKRYTY MAGAZYN DANYCH NA NOŚNIKU USB

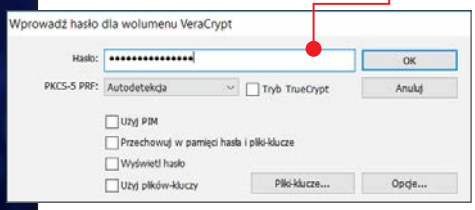
Korzystając z VeraCrypt, możemy również stworzyć przenośny sejf na pendrivie. Wystarczy, że będziemy postępować podobnie jak w przypadku porady dotyczącej tworzenia zaszyfrowanego wolumenu, z tą różnicą, że wybieramy opcję **Zaszyfruj bezsystemową partycję lub dysk**. W kolejnych krokach wystarczy wybrać nasz nośnik USB jako urządzenie do zaszyfrowania. **Uwaga!** Wszelkie dane z nośnika należy zabezpieczyć, ponieważ będzie on sformatowany przed zaszyfrowaniem.

Do odczytania zaszyfrowanego nośnika potrzebny jest zainstalowany program VeraCrypt. Gdy podłączymy nośnik do komputera z Windows, pojawi się informacja o formatowaniu (jeśli nie wyłączyliśmy opcji automatycznego montowania nośników), klikamy na **Anuluj**. Uruchamiamy program VeraCrypt, wybieramy nieużywaną literę z górnego okna i klikamy na **Podłącz automatycznie**.



Podajemy hasło i po chwili możemy korzystać z naszego nośnika jak z typowego urządzenia USB z danymi.

Jednak przed zakończeniem pracy i usunięciem nośnika z komputera koniecznie najpierw odłączmy go w programie VeraCrypt – jeśli tego nie zrobimy, ryzykujemy uszkodzenie danych w naszym sejfie.



TEST SZYBKOŚCI SZYFROWANIA

Szybkość, z jaką dysk zostanie zaszyfrowany, jest uzależniona od wydajności naszego komputera. Oto jak przetestować wydajność naszego procesora w szyfrowaniu danych przy wykorzystaniu różnych algorytmów. Jest to istotny test, bo pozwala na określenie, jaki algorytm należy wybrać, żeby szyfrowanie i deszyfrowanie oraz praca na zaszyfrowanym nośniku były jak najwydajniejsze.

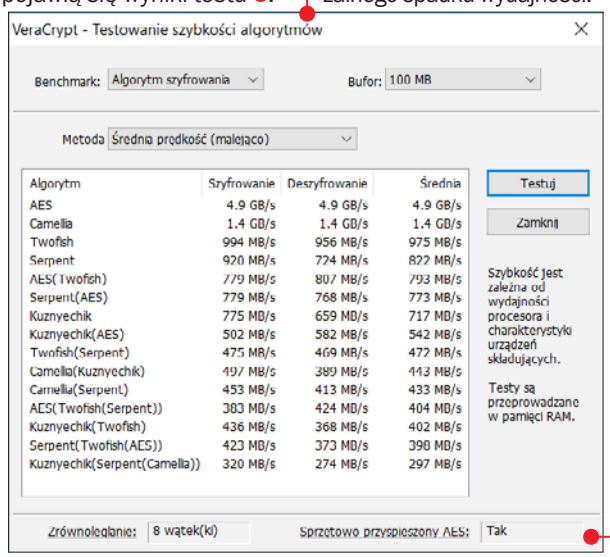
1 W głównym oknie klikamy na **Narzędzia**, **Testuj...**.

2 Zmieniamy ustawienia bufora na 100 MB i klikamy na **Testuj**.

3 Po chwili w oknie programu pojawią się wyniki testu.

Warto wiedzieć, że testy przeprowadzane są przy wykorzystaniu pamięci RAM, jedynym ograniczającym czynnikiem jest procesor. Niektóre procesory wspierają technologię sprzętowego przyspieszania algorytmu AES, która przyspiesza nawet osiem razy cały proces. Informacja, czy nasz procesor obsługuje przyspieszanie sprzętowe, jest umieszczona w prawym dolnym rogu okna.

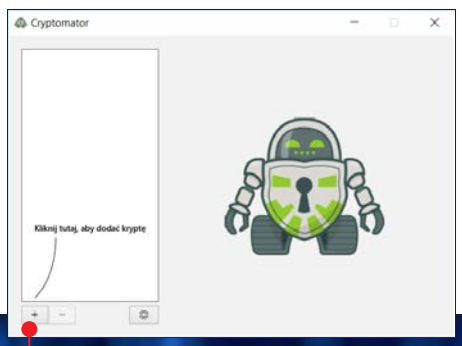
TrueCrypt może też wykorzystywać możliwość wielu rdzeni i wątków, liczba wykorzystywanych przez program wątków wyświetlana jest na dolnym pasku. Jeśli komputer wspiera tę technologię, możemy zaszyfrować cały dysk bez zauważalnego spadku wydajności.

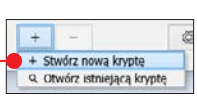


ZABEZPIECZAMY PLIKI W CHMURZE

Jeśli korzystamy na komputerze z dysków internetowych i synchronizujemy je z dyskiem lokalnym, warto rozważyć opcję szyfrowania danych na naszej maszynie. Silne hasło nie pozwoli nikomu uzyskać dostępu do naszych danych. W tym zadaniu świetnie sprawdzi się program **Cryptomator**.

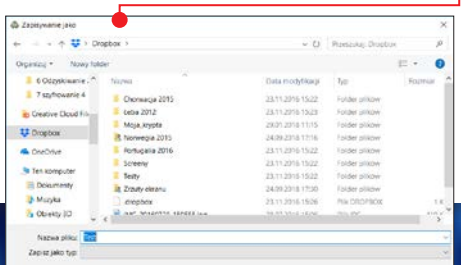
Jest to otwartoźródłowy program zaprojektowany z myślą o szyfrowaniu danych, jakie wgrywamy na dysk internetowy Dropbox, Dysk Google lub inny. Program szyfruje dane po stronie użytkownika algorytmem AES z 256-bitowym kluczem przed wysłaniem ich do chmury – pliki i foldery są ukrywane w tak zwanych kryptach, w których zostają ukryte również ich nazwy, rozmiary oraz struktura folderów. Możemy też zainstalować mobilną wersję programu na urządzeniu mobilnym po pobraniu z odpowiedniego sklepu.



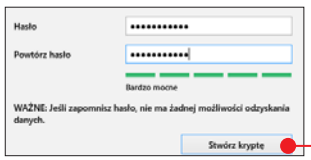


1 Po uruchomieniu programu klikamy na **+** w dolnym lewym rogu i wybieramy opcję **Stwórz nową kryptę**.

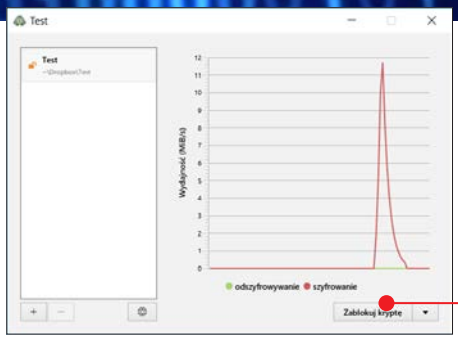
2 Przechodzimy do folderu na dysku, w którym synchronizowane są nasze dane w wybranej usłudze, na przykład Dropbox, nadajemy nazwę krypcie i klikamy na **Zapisz**.



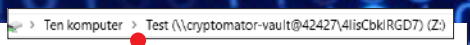
3 Teraz podajemy hasło do ochrony naszego sejfu i klikamy na **Stwórz kryptę**. Starajmy się stworzyć hasło, które zostanie rozpoznane jako bardzo mocne.



4 Następnie podajemy nasze hasło i klikamy na **Odblokuj kryptę**.

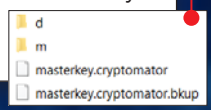


5 Otworzy się okno menedżera plików, będziemy mieli bezpośredni dostęp do naszego specjalnego schowka poprzez wirtualny nośnik. Możemy dowolnie przenosić pliki i foldery, które zostaną zaszyfrowane i zabezpieczone.



6 Po zakończeniu pracy klikamy na **Zablokuj kryptę**.

7 Nasze pliki są dostępne w chmurze, a jednocześnie są całkowicie bezpieczne. Do ich odszyfrowania konieczne jest użycie programu Cryptomator i podanie hasła. Krypty możemy tworzyć również na innych dyskach internetowych, jak OneDrive lub Google Drive.

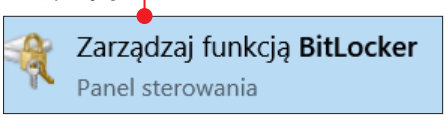


KORZYSTAMY Z FUNKCJI BITLOCKER

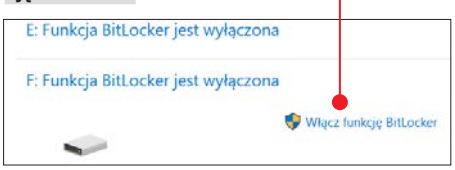
Dzięki tej funkcji systemu Windows można szyfrować całe dyski i partycje. **Uwaga!** Funkcja BitLocker nie jest dostępna dla użytkowników wersji Home Windows.

Szyfrujemy partycję z BitLocker

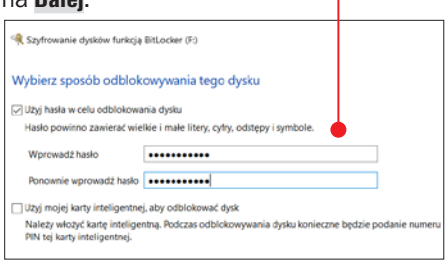
1 W polu wyszukiwania systemu Windows 10 wpisujemy **BitLocker** i klikamy na wyszukaną pozycję.



2 Teraz przy partycji, którą chcemy zaszyfrować, klikamy na polecenie **Włącz funkcję BitLocker**.

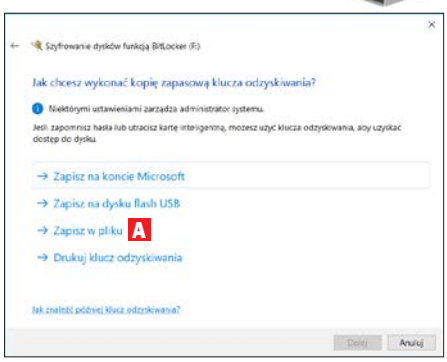


3 Następnie wybieramy opcję używania hasła, podajemy je dwukrotnie i klikamy na **Dalej**.

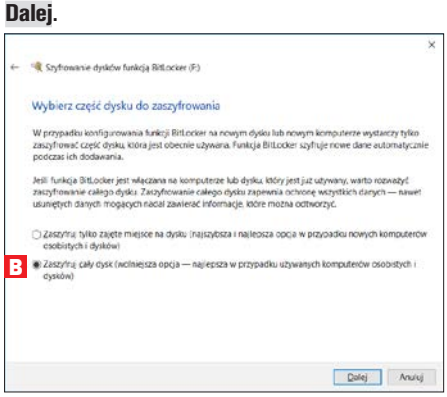


4 Następnie tworzymy kopię zapasową klucza odzyskiwania, klikamy na **Zapisz w pliku A**, wybieramy dowolną lokalizację na innej partycji i przechodzimy **Dalej**.

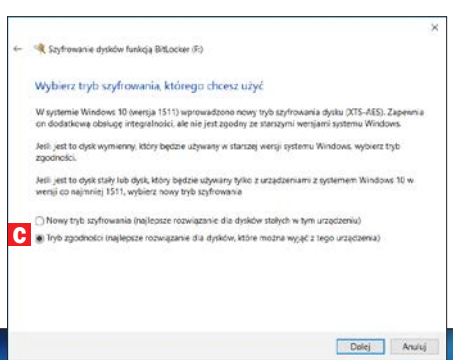
5 Następnie wybieramy opcję **Zaszyfruj cały dysk B** – w przypadku gdy nasz dysk był już wykorzystywany przez dłuższy czas – i klikamy na **Dalej**.



6 Jeśli szyfrujemy dysk, który będzie pracował również ze starszymi systemami, najlepiej wybrać opcję **Tryb zgodności C** i przejść **Dalej**.



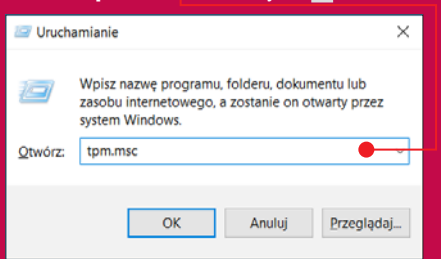
7 Na koniec klikamy na **Rozpocznij szyfrowanie**.



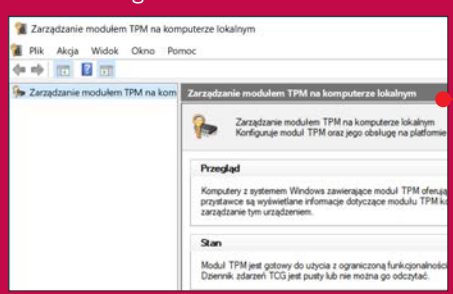
CZY NASZ KOMPUTER MA MODUŁ TPM

Moduł **TPM** (Trusted Platform Module) to specjalny układ, który może być wbudowany w płytę główną i służyć do przechowywania specjalnego klucza. Jeśli nasz komputer go nie ma, nie będziemy mogli zaszyfrować partycji systemowej bez dodatkowego nośnika USB.
Możemy łatwo sprawdzić, czy nasz komputer ma taki układ, czy też nie.

1 Wciskamy ⊞+R, wpisujemy w pole tekstowe **tpm.msc** i klikamy na **OK**.



2 Jeżeli pojawi się okno **Zarządzanie modułem TPM na komputerze lokalnym**, nasza maszyna jest wyposażona w taki moduł. Jeśli pojawi się informacja o błędzie, nasz komputer nie ma takiego modułu.



W większości przypadków może okazać się, że nie mamy takiego modułu, więc w poradzie obok zostało przedstawione szyfrowanie partycji niesystemowej. Jeśli zależy nam na zaszyfrowaniu dysku systemowego, cała procedura będzie bardziej złożona i będziemy potrzebowali dodatkowego nośnika USB.

W PRAKTYCE

ODZYSKIWANIE DANYCH

Dysk systemowy, dodatkowy, przenośny

Procedura odzyskiwania danych różni się znacząco w zależności od sprzętu, z którego dane chcemy odzyskać. Inaczej musimy postępować w przypadku plików usuniętych z dysku systemowego, dysku dodatkowego czy kart pamięci.

W przypadku dysku systemowego najważniejsze jest jak najszybsze wyłączenie zasilania sprzętu. Jest to ważne ze względu na niebezpieczeństwo nadpisania skasowanego pliku nowymi danymi przez system lub inne programy. Do odzyskania danych z takiego dysku przyda się drugi komputer lub specjalnie przygotowany bootowalny nośnik, który pomoże odzyskać dane (patrz strona obok).

W przypadku kart pamięci i dysków dodatkowych odzyskiwanie jest znacznie prostsze, ponieważ możemy po prostu zainstalować odpowiednie oprogramowanie do odzyskiwania danych na dysku systemowym, przeskanować nośnik i przywrócić pliki.

Co się dzieje, gdy usuwamy dane

Jeśli usunęliśmy dane, korzystając na przykład z klawisza delete, wtedy domyślnie zostały one przeniesione do Kosza systemowego i ich odzyskanie jest banalnie proste – polega na wejściu do folderu Kosz, kliknięciu na dany plik prawym przyciskiem myszy i wybranie opcji **Przywróć**.

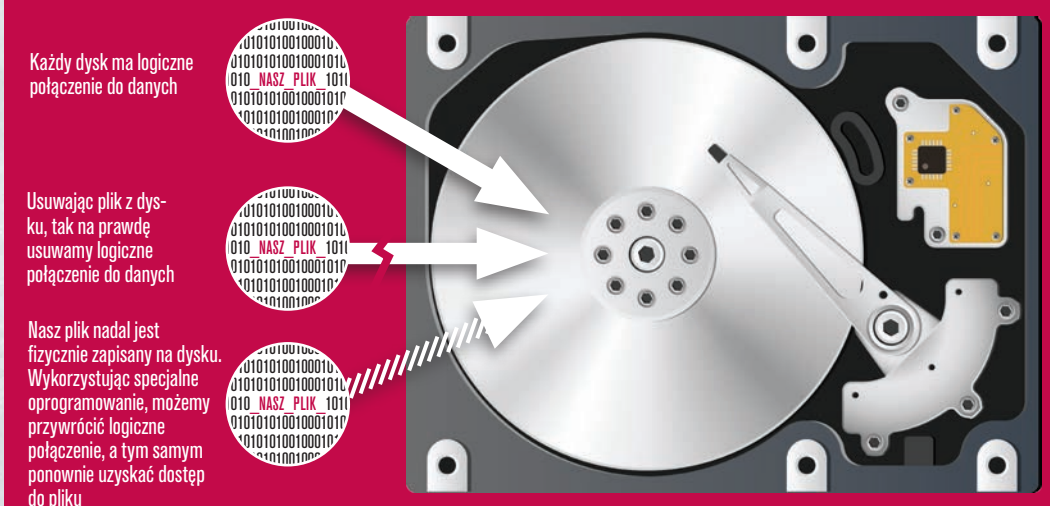
Jeżeli jednak usuniemy plik trwale, czyli na przykład wciśniemy kombinację klawiszy shift + delete i zatwierdzimy operację usuwania, wtedy plik znika z naszego dysku. Co dzieje się z nim tak naprawdę? Odpowiedź jest różna w zależności od typu nośnika.

Dyski HDD

Popularne dyski twarde charakteryzują się tym, że mają w środku talerze, które kręcą się z odpowiednią prędkością. W ich przypadku każdy odczyt i zapis danych odbywa się na ścieżkach, które podzielone są na sektory. Aby dysk działał możliwie jak najszybciej, tworzone są specjalne mapy ścieżek i sektorów. Dane zapisywane są do sektorów oznaczonych jako „wolne" przez specjalną flagę logiczną. Gdy trwale usuwamy jakiś plik w systemie Windows, do dysku dociera informacja o tym i sektory, które przechowywały dany plik, zostają oznaczone jako „wolne". Fizycznie dysk twardy nie usuwa zapisanych danych, ponieważ znacznie obniżyłoby to jego wydajność – prościej jest nadpisać zajęte wcześniej sektory.

Dzięki temu możliwe jest dość proste odzyskanie danych po ich „trwałym" usunięciu – wystarczy przywrócić odpowiednie logiczne połączenie, ponieważ dane nadal są na dysku. Pomogą nam w tym programy opisane na stronie 52.

CO TAK NAPRAWDĘ DZIEJE SIĘ NA DYSKU HDD, GDY USUWAMY PLIK W SYSTEMIE WINDOWS



Dyski SSD

Coraz więcej osób korzysta z dysków SSD – półprzewodnikowych lub stałych. Nie mają one żadnych części ruchomych. Ich największą zaletą jest znacznie wyższa wydajność w stosunku do HDD. Proces kasowania danych na takim dysku wygląda zupełnie inaczej. W momencie trwałego usunięcia pliku w systemie Windows dane na dysku SSD również są fizycznie wymazywane, ponieważ tego typu nośniki szybciej zapisują dane na pustej przestrzeni. Odzyskanie danych z tego typu nośników mogłoby być więc po prostu niemożliwe. Aby temu zaradzić, obecnie nośniki SSD korzystają ze specjalnych banków pamięci, które zapisują mapy struktur blokowych. Mogą one być wykorzystane przez specjalne oprogramowanie do odzyskiwania danych użytkownika. **kd**

Omyłkowe usunięcie, awaria prądu, zepsucie się nośnika, atak wirusów – przyczyn utraty danych może być wiele. Czasem udaje się na szczęście odzyskać utracone pliki. Przeczytajmy, ***na czym polega przywracanie i w jaki sposob je przeprowadzić***

WYJMUJEMY DYSK SYSTEMOWY Z LAPTOPA

W przypadku komputera stacjonarnego wyjęcie dysku nie powinno stanowić problemu: rozkręcamy obudowę i odpinamy nośnik systemowy. W laptopach może być to znacznie bardziej skomplikowane. Wszystko zależy od modelu naszego urządzenia. Większość nowszych laptopów na spodzie ma specjalną klapkę oznaczoną jako **HDD**, pod którą znajduje się dysk twardy. Wymontowany dysk możemy podłączyć bezpośrednio do innego komputera poprzez interfejs SATA lub włożyć do obudowy na dyski przenośne i podłączyć poprzez interfejs USB. Musimy upewnić się, że komputer nie uruchomi się, korzystając z dysku, z którego chcemy odzyskać dane (w Boot Menu wybieramy odpowiedni nośnik do bootowania – patrz porada niżej). Potem możemy przejść do odzyskiwania danych, wykorzystując na przykład programy, które znajdziemy na płycie dołączonej do tego wydania.

ODZYSKUJEMY DANE Z DYSKU SYSTEMOWEGO BEZ WYJMOWANIA GO

Jeśli nie chcemy wyjmować dysku, możemy skorzystać z alternatywnej metody odzyskiwania, wykorzystując bootowalny nośnik tworzony w programie **Lazesoft Recovery Suite** (DVD-KOD: **033**).

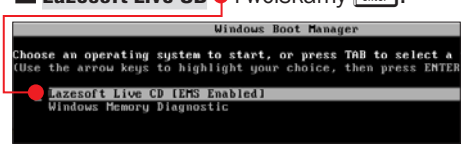
Lazesoft Recovery Suite to kompletny pakiet do odzyskiwania danych. Pozwala też między innymi na archiwizację danych, naprawę mechanizmu rozruchu systemu czy odzyskiwanie haseł. Najciekawszym rozwiązaniem jest jednak dysk rozruchowy, który pozwala odzyskać dane nawet z dysku systemowego bez przenoszenia go do innego komputera. Aby utworzyć nośnik bootowalny, wystarczy kliknąć w oknie programu na **Burn CD/USB Disk** i postępować według wskazówek kreatora.

Uwaga! Ponieważ po skasowaniu ważnych danych z dysku systemowego nie możemy uruchamiać z niego systemu, taki nośnik należy utworzyć na innym komputerze lub przygotować go wcześniej, na wszelki wypadek.

KORZYSTAMY Z DYSKU RATUNKOWEGO

1 Uruchamiamy komputer, korzystając z bootowalnego nośnika. W tym celu podłączamy nośnik i po wyświetleniu logo producenta komputera naciskamy klawisz włączający menu rozruchowe, czyli Boot Menu. Informacja, jaki to klawisz, powinna być widoczna u dołu ekranu. Najczęściej jest to F8, F9, F11, F12, esc. W Boot Menu wybieramy nośnik USB.

2 Na ekranie Boot Menu wybieramy opcję **Lazesoft Live CD** i wciskamy enter.



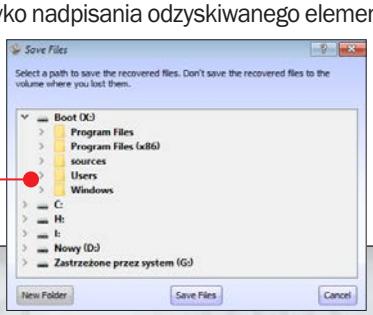
3 Po chwili załaduje się ekran narzędzia ratunkowego. Klikamy na pomarańczowy kafelek – **Data recovery**.

4 Wskazujemy dysk, z którego chcemy spróbować odzyskać dane, i klikamy na **OK**.

5 Wybieramy tryb pracy programu najbardziej dopasowany do naszych potrzeb – jeśli chcemy odzyskać skasowane pliki, klikamy na **Undelete**. Wybieramy partycję, którą chcemy przeskanować, i klikamy na **Start search**.

6 Następnie zaznaczamy pliki, które chcemy odzyskać, i klikamy na **Save Files**.

7 Pliki możemy zapisać bezpośrednio na bootowalnym nośniku, innych dyskach i partycjach. **Uwaga!** Nie zapisujemy danych, które odzyskujemy, na tym samym dysku, gdyż jest ryzyko nadpisania odzyskiwanego elementu.



Fot. Maksim Kabakou/123rf.com

TRIKI DO PROGRAMÓW
NAJLEPSZE PROGRAMY DO ODZYSKIWANIA PLIKÓW

ODZYSKIWANIE

*Na płycie dołączonej do tego wydania znajdziemy między innymi **pakiet narzędzi do odzyskiwania danych**. Poznajmy te programy i dowiedzmy się, jak z nich korzystać*

Zdarza się, że dysk lokalny czy przenośny ulega awarii, która może pozbawić nas dostępu do danych. A czasem sami przez nieuwagę skasujemy pliki, które po pewnym czasie okazują się potrzebne. Na szczęście utracone dane możemy spróbować odzyskać za pomocą specjalnych programów.

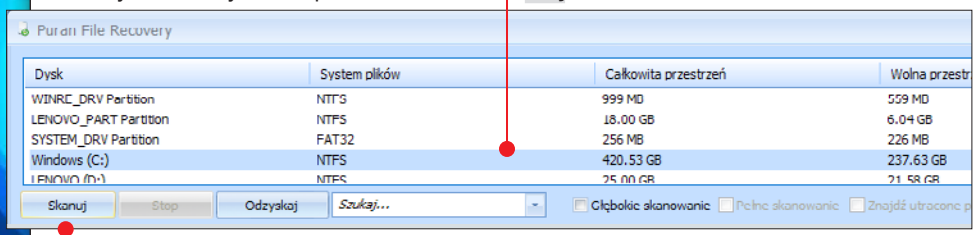
Czas ma znaczenie

Niezależnie od tego, w jaki sposób utraciliśmy swoje pliki, czas, jaki ułynął od ich utraty do próby odzyskania, ma wpływ na powodzenie tego procesu. Dlaczego? Jeżeli usunęliśmy dane z dysku twardego, a następnie z niego korzystaliśmy, w miejscu, w którym się one znajdowały, zostają zapisane inne dane. A to może uniemożliwić odzyskanie tych utraconych. Aby zwiększyć szanse na przywrócenie danych, nie powinniśmy zapisywać nowych plików na danym nośniku przed próbą odzyskania. **kj**

ODZYSKIWANIE DLA POCZĄTKUJĄCYCH

Puran File Recovery (DVD-KOD: **049**) to narzędzie, które można polecić początkującym użytkownikom, chcącym spróbować odzyskać utracone dane.

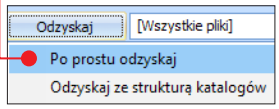
1 Po uruchomieniu programu należy jedynie wskazać odpowiedni dysk lub partycję, którą chcemy przeskanować w poszukiwaniu możliwych do odzyskania plików.



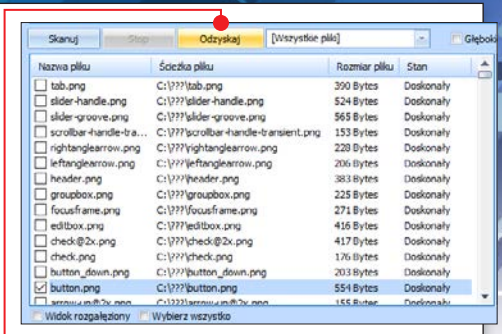
2 Po dokonaniu wyboru klikamy na **Skanuj**, aby rozpocząć poszukiwania.

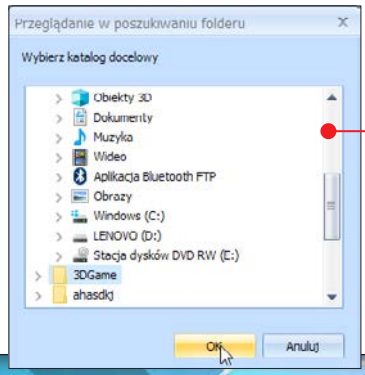
3 Po zakończeniu skanowania program wyświetli listę odnalezionych plików. Pliki te oznaczone są lokalizacją, w jakiej się znajdowały, rozmiarem, a także stanem. Ostatni parametr informuje nas o tym, czy plik, który będziemy chcieli odzyskać, nie uległ znacznemu zniszczeniu i czy próba jego odzyskania ma w ogóle szanse na powodzenie. Aby odzyskać odszukany plik (lub pliki), zaznaczamy go i klikamy na polecenie **Odzyskaj**.

4 Dalej wybieramy opcję **Po prostu odzyskaj**.



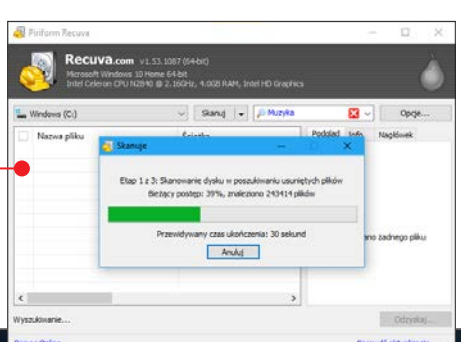
5 W kolejnym kroku wskazujemy, gdzie chcemy zapisać odzyskiwany plik. Należy wskazać lokalizację na innym nośniku niż ten, z którego odzyskujemy dane.

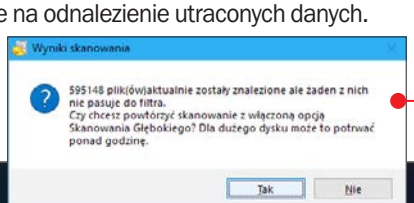




GŁĘBOKIE WYSZUKIWANIE PLIKÓW DO ODZYSKANIA

Recuva (DVD-KOD: **050/051** PORTABLE) to narzędzie, które potrafi odszukać i odzyskać pliki usunięte z dysku. Po wybraniu dysku, z którego odzyskujemy pliki, a także (ewentualnie) rodzaju plików i kliknięciu na **Skanuj** – przeprowadzone zostaje poszukiwanie. Zdarza się jednak, że może ono nie zakończyć się powodzeniem. Pozwólmy jednak programowi Recuva na ponowne skanowanie – tym razem z wykorzystaniem **Skanowania Głębokiego**, o którego uruchomienie zostaniemy zapytani po przeprowadzeniu zwykłego skanowania. Odpowiadamy twierdząco – a Recuva wykonuje kolejne skanowanie, które jest znacznie dokładniejsze od pierwszego, co zwiększa szanse na odnalezienie utraconych danych.



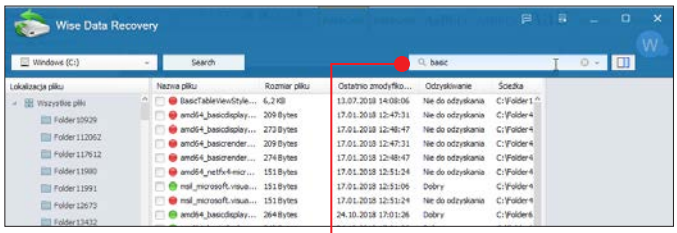


DANYC

NA NASZYM **DVD**

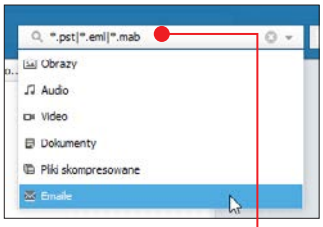
ODZYSKIWANIE **WIADOMOŚCI E-MAIL**

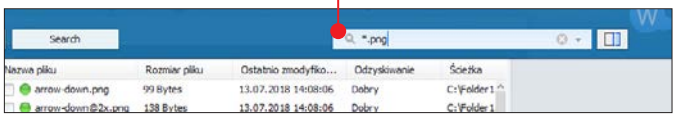
Wise Data Recovery (DVD-KOD: **072**) to oprogramowanie do odzyskiwania plików, które oferuje wygodny system filtrowania wyszukanych danych możliwych do odzyskania. Po przeprowadzeniu skanowania



możemy wpisać słowa kluczowe w wyszukiwarce ●, by przefiltrować listę wyników. W pole wyszukiwania można wpisywać też formaty plików – w formie ***.rozszerzenie** – co dla plików w formacie PNG wyglądałoby następująco: ***.png** ●.

Możemy również rozwinąć listę, aby wybrać zestaw formatów z danej kategorii. Wśród kategorii znajduje się też Email. Ponieważ programy pocztowe przechowują wiadomości w formie plików na dysku – również możemy je odzyskać. Wybranie opcji **Email** filtruje wyniki wyszukiwania do zbioru formatów ●, w jakich programy pocztowe zapisują e-maile.





ZAAWANSOWANE ODZYSKIWANIE **OBSŁUGIWANE WIERSZEM POLECENIA**

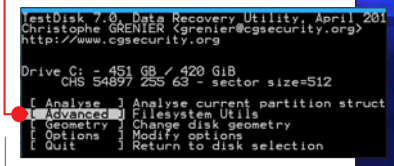
TestDisk (DVD-KOD: **058**) to narzędzie bez warstwy graficznej – obsługujemy je przez Wiersz polecenia, klawiszami strzałek i klawiszem enter. Program stworzono z myślą o odzyskiwaniu partycji i naprawianiu tablic partycji na dyskach twardych, nośnikach SSD, pamięciach USB, macierzach RAID.

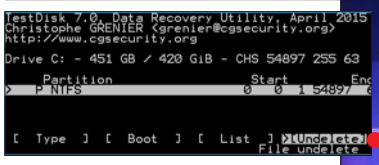
1 Aby wykonać odzyskiwanie danych z partycji NTFS, po uruchomieniu TestDisk wybieramy opcję **Create** ●, by utworzyć plik z informacją o danych na dysku.

2 Wskazujemy dysk lub partycję ●, z której chcemy odzyskać dane.

3 Program wykrywa typ tablic partycji na wybranym przez nas dysku – nie zmieniamy ustawień ● i przechodzimy dalej.

4 Wybieramy **Advanced** ●. Naciskamy klawisz →, by przejść do opcji **Undelete** ●.





5 Program przetwarza dane i po pewnym czasie wyświetla listę usuniętych plików możliwych do odzyskania. Wybieramy z listy interesujący nas plik i naciskamy klawisz C. Plik zostaje skopiowany, a my zostaniemy poproszeni o wskazanie lokalizacji, w której ma zostać zapisany odzyskany plik.

BOOTOWALNE NARZĘDZIE DO ODZYSKIWANIA

Lazesoft Recovery Suite (DVD-KOD: **033**) to cały pakiet narzędzi do odzyskiwania danych, tworzenia kopii zapasowych, umożliwiających w razie awarii przywracanie danych, i do naprawiania uszkodzonego systemu. Lazesoft Recovery Suite Professional działa jako nośnik ratunkowy. Aby móc korzystać z funkcji programu, najpierw za pomocą kreatora, który poprowadzi nas krok po kroku, musimy utworzyć bootowalny dysk CD lub nośnik USB. W razie awarii będziemy mogli uruchomić z niego komputer, a potem:

A przywrócić system w wypadku problemów z rozruchem Windows,

B odzyskać dane z dysków twardych, kart pamięci lub dysków flash utracone w wyniku przypadkowego usunięcia, formatowania lub uszkodzenia,

C stworzyć obraz dysku lub partycji, by móc przywrócić system i dane w wypadku awarii, tworzyć i formatować partycje czy wymazać dysk,

D odzyskać lokalne hasło systemu Windows.

Aby utworzyć bootowalny nośnik z Lazesoft Recovery Suite, klikamy na **Burn CD/USB Disk** ●.

Więcej o programie przeczytamy na stronie 51.

Fot. Kran Kanthawong/123rf.com

TRIKI
DO PROGRAMÓW
BEZPIECZNA PIASKOWNICA

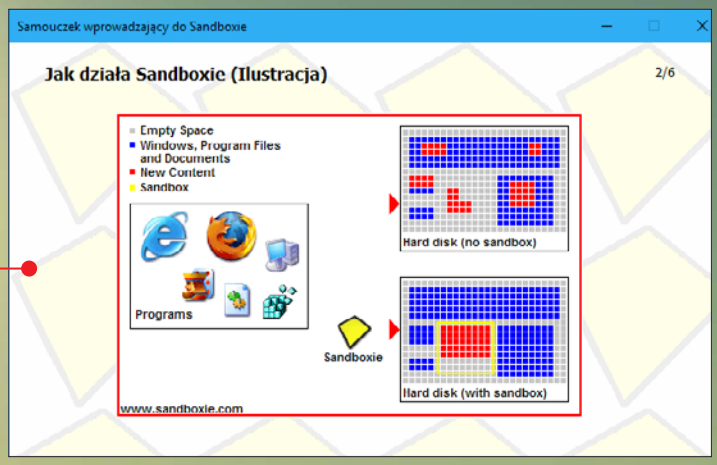
SANDBOKSOWA

Sandbox, czyli piaskownica, to odizolowana przestrzeń, wewnątrz której można ***uruchamiać programy, których bezpieczeństwa nie jesteśmy pewni lub które mogą być źródłem zagrożenia****. Poznajmy to rozwiązanie*

Uruchomione w komputerze aplikacje mają dostęp do jego zasobów. Mogą zbierać informacje o użytkowniku, wprowadzać zmiany do ustawień czy też skanować zawartość dysku. Tego typu uprawnienia są chętnie wykorzystywane przez twórców oprogramowania, nie tylko złośliwego.

Czym jest sandboksowanie

Czy możemy uchronić się przed zagrożeniami, jakie stwarzają progamy działające w komputerze? Jednym ze sposobów jest utworzenie na dysku całkowicie odizolowanej przestrzeni, nazywanej piaskownicą (ang. sandbox), wewnątrz której będzie można uruchamiać programy. Aplikacje uruchomione w takiej przestrzeni nie będą miały dostępu do całego dysku – a co za tym idzie, złośliwe oprogramowanie nie wydostanie się poza ograniczony obszar. Jak działają piaskownice, możemy dowiedzieć się na przykładzie programu **Sandboxie** (DVD-KOD: **053**), który znajdziemy na płycie dołączonej do tego wydania. To aplikacja, która może uruchamiać inne programy w odizolowanym środowisku. W samouczku Sandboxie pokazano, jak na dysku twardym rozmieszczają się dane powiązane z nowo instalowanym programem, gdy jest piaskownica i gdy jej nie ma.



Kiedy używać piaskownicy

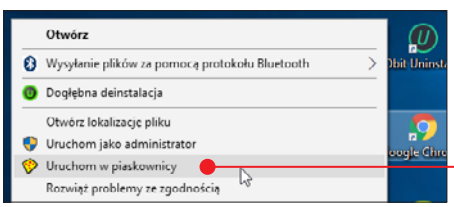
Oczywiście, w piaskownicy nie trzeba trzymać wszystkich aplikacji. Jest jednak kilka typów programów, które warto uruchamiać w sandboxie. Należą do nich przeglądarki internetowe i programy pocztowe – to dwa podstawowe źródła nowych plików pojawiających się na naszych dyskach. Mogą to być pliki pobierane poprzez odnośniki na stronach internetowych czy też załączniki z wiadomości e-mail. Może być w nich ukryte złośliwe oprogramowanie.

Piaskownice są także doskonałym sposobem na zwiększenie prywatności. Instalowane przez nas programy mogą ingerować w prywatność – choćby zbierając dane o zainstalowanym na urządzeniu oprogramowaniu. Producenci dane te wykorzystują w celach reklamowych i statystycznych, aby lepiej dopasowywać swoją ofertę do użytkowników. Jeśli aplikacja, która gromadzi dane, będzie uruchomiona w piaskownicy, nie będzie miała dostępu do tego, co jest poza wydzielonym obszarem – a co za tym idzie, nie będzie mogła sprawdzić, jakie inne aplikacje zainstalowane są na naszym urządzeniu. **kj**

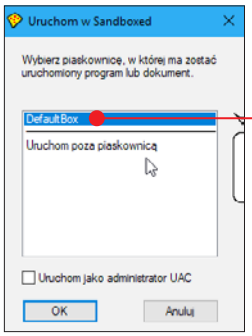
JAK URUCHAMIAĆ APLIKACJE W PIASKOWNICY

Aby móc uruchomić jakiś program w piaskownicy, niezbędne będzie nam oprogramowanie, które taki wydzielony obszar będzie mogło utworzyć. Dobrze sprawdzi się tutaj właśnie Sandboxie.

1 Po instalacji aplikacja ta integruje się z menu kontekstowym. Dzięki temu, chcąc uruchomić wybraną aplikację w wydzielonym obszarze, wystarczy kliknąć na jej ikonę prawym przyciskiem myszy, aby wyświetlić menu kontekstowe.

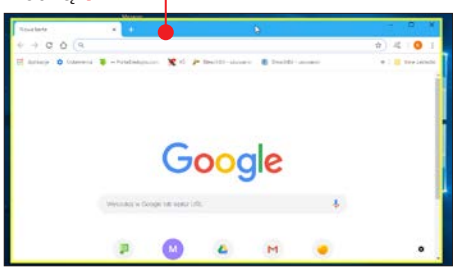


2 W menu znajduje się opcja **Uruchom w piaskownicy** – klikamy na nią.



3 Następnie program prosi nas o wybór, w której z piaskownic mamy uruchomić aplikację. Domyślnie do wyboru mamy tylko jedną piaskownicę – **DefaultBox**.

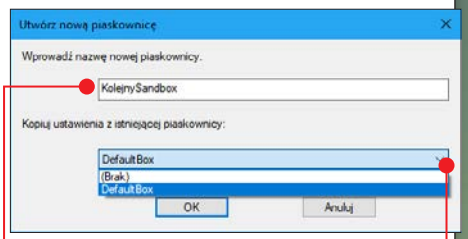
4 Uruchomiona w piaskownicy aplikacja podczas użytkowania różni się dla nas tylko tym, że jej okno jest otoczone żółtą obwódką.



NIE PROGRAMÓW

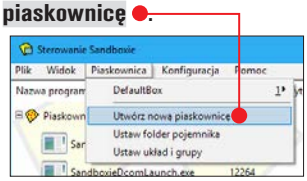
JAK TWORZYĆ NOWY IZOLOWANY OBSZAR

Na początku korzystania z programu mamy tylko jedną piaskownicę – DefaultBox. Gdy uruchomimy w niej kilka programów, będą dzielić między sobą ten sam obszar (czyli mogą też komunikować się między sobą).



1 Aby utworzyć kolejne izolowane obszary, które są od siebie niezależne, musimy przejść do okna **Sterowania Sandboxie** (patrz ramka obok).

2 Tam, z menu głównego rozwijamy pozycję **Piaskownica** i wybieramy opcję **Utwórz nową piaskownicę**.

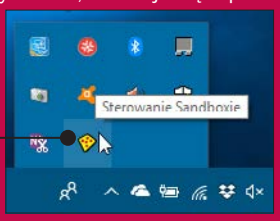


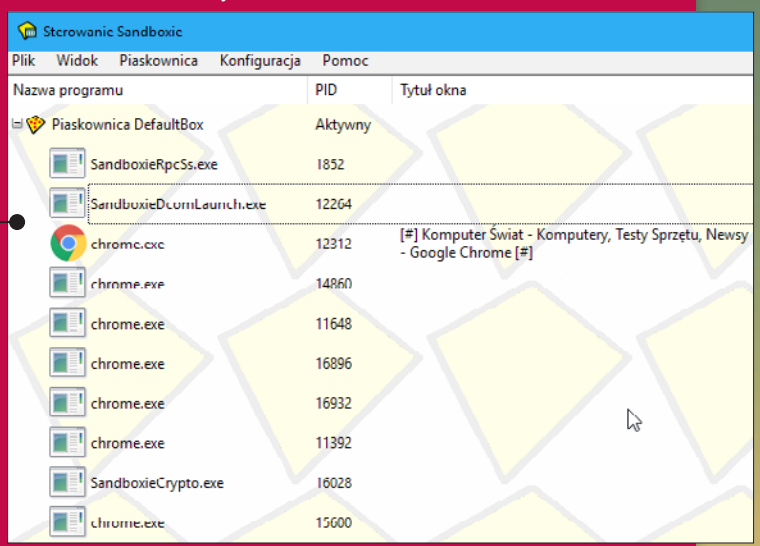
3 W nowym oknie możemy podać nazwę nowej piaskownicy. W polu poniżej nazwy powinniśmy zmienić opcję **(Brak)** na **DefaultBox**, aby nowa piaskownica utworzyła się z ustawieniami, jakie program Sandboxie wybrał dla nas przy tworzeniu domyślnej piaskownicy.

4 Po zatwierdzeniu utworzenia piaskownicy, gdy będziemy uruchamiać za pomocą Sandboxie kolejne programy, będziemy mieli do wyboru nowy izolowany obszar.

STEROWANIE SANDBOXIE

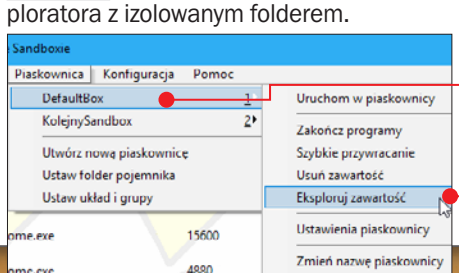
Obsługa programu Sandboxie nie ogranicza się jedynie do prostego uruchamiania aplikacji. Mamy większy wpływ na to, co dzieje się w programie. Aby mieć naszą piaskownicę pod kontrolą, należy dostać się do okna **Sterowanie Sandboxie**. Ikonę, która je otwiera, znajdziemy w zasobniku systemowym. Po wyświetleniu okna sterowania zobaczymy procesy, które odbywają się w naszej piaskownicy, podobnie jak w Menedżerze zadań systemu Windows.



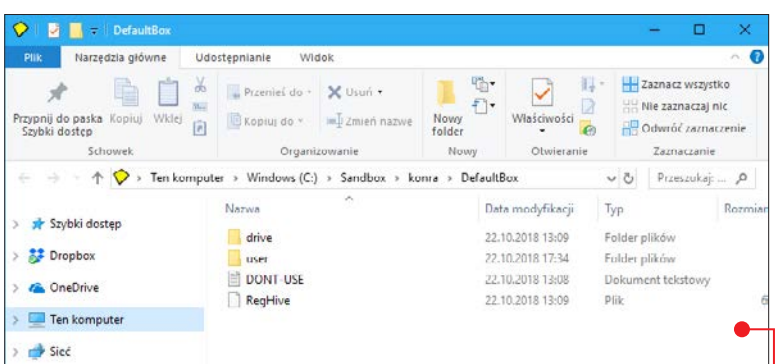


JAK DOSTAĆ SIĘ DO PLIKÓW

Pliki zapisywane na naszym komputerze przez programy uruchomione w piaskownicy również są umieszczane w izolowanym obszarze. Możemy je jednak przenosić poza sandbox. W tym celu przez okno **Sterowanie Sandboxie** musimy dostać się do okna Eksploratora z izolowanym folderem.



1 Z menu głównego rozwijamy pozycję **Piaskownica** i najeżdżamy kursorem na piaskownicę, do której chcemy się dostać.



2 Wyświetlona zostanie lista opcji dotyczących wybranej piaskownicy – wybieramy **Eksploruj zawartość**.

3 Wyświetlone zostanie okno Eksploratora z lokalizacją izolowanego folderu – z którego możemy przenosić zawartość w inne miejsca.

Fot. Kirsty Pargeter/123rf.com

TRIKI
DO PROGRAMÓW
MENEDŻERY HASEŁ

SEJFY NA HASŁ

*Hasła do logowania się do usług i kont powinny być różne, trudne do odgadnięcia, a przy tym – **nie możemy ich zapomnieć ani pomylić**. Na szczęście są menedżery haseł*

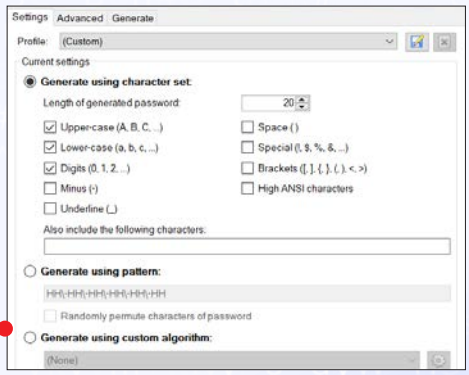
Dzisiejszy internet to przebogate źródło informacji, rozrywki, a także często miejsce pracy. Mało kto korzysta dziś z tylko jednego konta pocztowego lub jednej wybranej usługi sieciowej. A to sprawia, że liczba haseł, które musimy zapamiętać, staje się dla nas trudna. Co więcej, hasłami, kodami dostępowymi chronimy również dostęp do usług finansowych, a naruszenie ich bezpieczeństwa może mieć poważne dla nas skutki. Jak sobie poradzić z tysiącem haseł do zapamiętania i ułatwić wypełnianie czasem rozbudowanych formularzy? Jest na to prosta recepta – menedżery haseł. Można je podzielić na dwie grupy: takie, które działają lokalnie – jak KeePass, oraz takie, które przechowują wszystkie dane w chmurze – jak Last Pass. Przyjrzymy się funkcjonowaniu tych narzędzi. **kż**

CZY WARTO KORZYSTAĆ Z MENEDŻERA HASEŁ

Jeden z najlepszych komputerowych hakerów, Kevin Mittnick, twierdzi, że menedżer haseł nic nie da, gdy będziemy stosować proste frazy (czyli zbyt krótkie), łatwe do odgadnięcia przez algorytmy oprogramowania łamiącego hasła.
Należy pamiętać, że aby menedżer haseł stał się pożyteczny, musimy zabezpieczyć dostęp do niego skomplikowanym hasłem, czyli takim, które nie tylko zawiera kombinację różnych znaków, ale łączy je w sposób nieprzewidywalny i jest długie (najlepiej 20 i więcej znaków). Może to być oryginalne zdanie, dla nas łatwe do zapamiętania, dla hakera niemożliwe do złamania.
Także hasła, które zabezpieczamy w takim sejfie, powinny być skomplikowane i różnić się od siebie. Skoro korzystamy z menedżera – możemy tworzyć trudne hasła bez obawy, że je zapomnimy.

KEEPASS

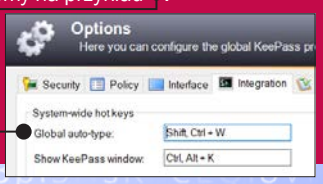
KeePass to najpopularniejsza i jedna z najlepszych aplikacji – menedżerów haseł. Wyróżnia się dobrze zorganizowaną bazą, w której przechowywane są posortowane dane dostępowe do witryn, klucze do aplikacji czy PIN-y. Dostęp do bazy można zabezpieczyć kluczem, który przechowywany jest na zewnętrznym nośniku. KeePass może generować trudne do odgadnięcia hasła. Program maksymalnie upraszcza wprowadzanie danych, utrudnia ich przypadkowe podejrzenie na ekranie czy przez analizę zawartości schowka, dba też o blokowanie dostępu do bazy haseł, gdy program jest długo włączony. Możemy używać go



w wersji stacjonarnej (DVD-KOD: **024**) lub przenośnej (DVD-KOD: **026**). W tym drugim przypadku warto zainstalować KeePass na pendrivie, który posłuży wtedy jako klucz dostępowy.

KONFLIKT SKRÓTÓW KLAWIATUROWYCH

Domyślny w KeePass skrót klawiaturowy do wprowadzania danych z bazy haseł jest taki sam jak skrót dla litery „ą". By go zmienić, klikamy na **Tools**, **Options** i na zakładce **Integration** wpisujemy na przykład .



NOWA BAZA HASEŁ Z KLUCZEM NA PENDRIVE

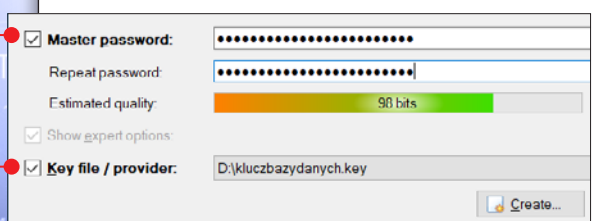
Prace z KeePass zaczynamy od stworzenia bazy haseł.

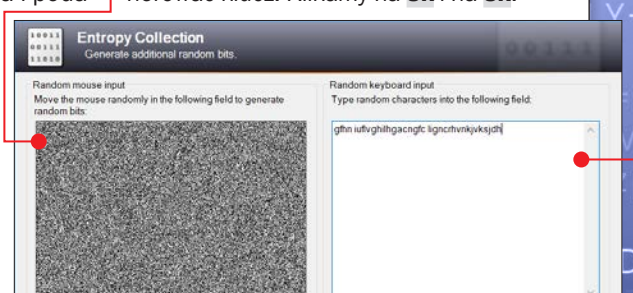
1 Wciskamy skrót [ctrl] + [N]. Klikamy na **OK** i wskazujemy lokalizację pliku bazy danych. Klikamy na **Zapisz**.

2 W kolejnym oknie podajemy hasło główne. Zaznaczamy pola wyboru i klikamy na **Create**. Wskazujemy lokalizację na pendrivie podłączonym do komputera i podajemy nazwę pliku klucza. Klikamy na **Zapisz**.

3 Teraz, by zadziałała baza haseł, konieczne jest nie tylko wpisanie hasła głównego, ale też podłączenie do komputera pendrive'a z plikiem-kluczem, który stworzyliśmy w punkcie **2**.

4 Klikamy na **OK**. W kolejnym oknie wpisujemy dowolny ciąg znaków w pole , a nad polem wykonujemy ruchy myszą, by wygenerować klucz. Klikamy na **OK** i na **OK**.





LA

LAST PASS

Praktycznie każda przeglądarka internetowa oferuje mechanizm przechowywania haseł i ich synchronizacji pomiędzy urządzeniami. To przydatne rozwiązanie, ale też problematyczne. Dla każdej przeglądarki musimy tworzyć nową bazę haseł (czasem pomaga opcja importu), a kontrolowanie zgromadzonych haseł nie jest zbyt wygodne. Poza tym przeglądarkowy menedżer haseł nie zawsze oferuje opcję wypełniania formularzy jak zewnętrzne narzędzia.

Jeśli jesteśmy zwolennikami przechowywania bazy haseł w chmurze, do której mamy dostęp z przeglądarki dowolnego typu, warto sięgnąć po aplikację Last Pass (DVD-KOD: **032**). Instalator dodaje do przeglądarek na komputerze rozszerzenia, które umożliwiają im synchronizację haseł z jedną centralną bazą przechowywaną w sieci.

NA DVD TAKŻE:

1Password (DVD-KOD: **001**) – jeden z najbardziej rozbudowanych menedżerów haseł i informacji poufnych. Wszystkie zapamiętane przez program informacje są szyfrowane silnym algorytmem AES-256 i zabezpieczone hasłem głównym. Dane możemy synchronizować pomiędzy różnymi urządzeniami.

KeePassX (DVD-KOD: **027**) – menedżer haseł oparty na kodzie źródłowym popularnego KeePassa. KeePassX przechowuje loginy, hasła, adresy internetowe oraz inne informacje w zaszyfrowanej bazie danych. Dostęp do bazy danych uzyskujemy, podając hasło oraz opcjonalny plik-klucz.

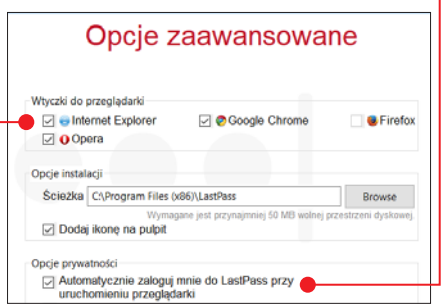
KeePassXC (DVD-KOD: **028 / 029 / 030** 32- / 64-BIT / PORTABLE) – otwarto-źródłowy i wieloplatformowy menedżer haseł, oparty na kodzie programu KeePassX. Oferuje rozszerzone i ulepszone funkcje pierwowzoru. Dane szyfrowane są algorytmem AES, Twofish lub Cha-Cha20. Zawiera generator silnych haseł.

Password Safe (DVD-KOD: **044 / 045** 32- / 64-BIT) – prosty program do bezpiecznego przechowywania haseł i innych poufnych informacji w zaszyfrowanej bazie danych (jednej lub kilku), którą można przenosić pomiędzy komputerami. Nasze dane zabezpieczone są hasłem głównym.

PIERWSZE URUCHOMIENIE

Przy pierwszym uruchomieniu Last Pass musimy wykonać kilka kroków, by korzystać z narzędzia.

1 Najpierw określamy, do jakich przeglądarek ma zostać dodane rozszerzenie Last Pass. Możemy potem samodzielnie doinstalować rozszerzenie. Warto też zaznaczyć pole wyboru.



2 Następnie klikamy na **Zainstaluj Last Pass**, a potem na **Stwórz nowe konto**. Będzie ono konieczne do przechowywania haseł w sieci. Wypełniamy wymagane pola i klikamy na **Załóż konto**.

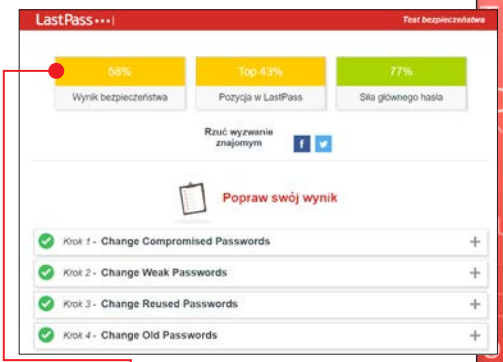
3 Last Pass zaproponuje import haseł z komputera do chmury (krypty). Po tej operacji dostęp do haseł uzyskamy poprzez wtyczkę Last Pass w przeglądarce, natomiast hasła zapisane w komputerze zostaną usunięte. Potwierdzamy operację, klikając na **Import**. Wybieramy **Nie, dziękuję**, gdy chcemy w Last Pass stworzyć nową bazę.

WERYFIKACJA HASEŁ

Po zaimportowaniu haseł do Last Pass warto ocenić ich siłę i w razie czego dokonać zmian lub wygenerować nowe za pomocą narzędzia **Generuj nowe hasło** w menu wtyczki Last Pass.

1 Uruchamiamy wtyczkę Last Pass, klikając na jej ikonę na pasku narzędziowym przeglądarki. Logujemy się – dla bezpieczeństwa hasło główne nie powinno być zapamiętywane (pole **Pamiętaj hasło** musi być niezaznaczone).

2 W menu wtyczki klikamy na **Więcej opcji** i **Test bezpieczeństwa**. Otworzy się witryna sieciowa, w której klikamy na **Pokaż mój wynik**.



3 W polu widnieje ocena poziomu bezpieczeństwa haseł. Inny kolor niż zielony oznacza, że warto poprawić hasła. Przewijamy stronę do **Wyniki szczegółowe**, gdzie podane są oceny dla każdego hasła. Poprawiamy te, które są uznane za słabe (warto, by poziom bezpieczeństwa przekraczał 85–90 procent).

KONTO RATUNKOWE

Mimo najszczerszych chęci możemy zapomnieć hasła głównego (nie należy go nigdzie zapisywać). W takiej sytuacji pomocą będzie zaufana osoba, dla której przygotujemy konto ratunkowe.

1 Z menu wtyczki Last Pass wybieramy **Open my vault**. Otworzy się witryna z listą przechowywanych w sieci haseł. Klikamy na **Dostęp awaryjny**, a potem na **Give emergency access**.

2 Otworzy się okno, w którym podajemy e-mail zaufanej osoby. Będzie ona mogła

stworzyć sobie konto i hasło, którym może zażądać ograniczonego awaryjnego dostępu do bazy haseł. Na liście określamy, jak szybko otrzyma ona dostęp po wysłaniu żądania dostępu. Klikamy na **Send invite**.

3 Tryb awaryjnego dostępu pozwala otworzyć dostęp do naszej bazy haseł.

Fot. Alexander Atkishkin/123rf.com

TRIKI
DO PROGRAMÓW
MICROSOFT
NA ANDROIDZIE

APLIKACJE MICROSOFTU *NA SMARTFONACH Z ANDROIDEM*

Na komputerach królują programy Microsoftu, a na smartfonach najpopularniejszy jest system Android i aplikacje tworzone na ten system. ***Można jednak pogodzić oba te światy*** *i ułatwić sobie pracę. Poznajmy aplikacje Microsoftu na Androida*

Smartfony z linii Lumia z systemem Windows to już odległa przeszłość z perspektywy branży mobilnej. Ale to, że nie ma już smartfonów z Windows, wcale nie oznacza, że używając smartfona, nie możemy korzystać z zalet oprogramowania Microsoftu. Wręcz przeciwnie – każdy smartfon z Androidem jest też trochę microsoftowy, bo można uruchomić na nim aplikacje tego producenta.

Przyjrzyjmy się, jakie to mogą być aplikacje i do czego nam się przydadzą.

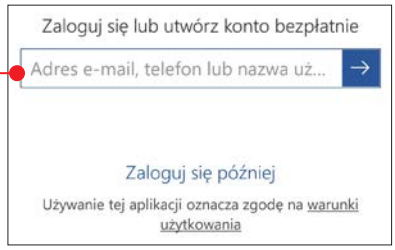
Jak instalować aplikacje Microsoftu

By zainstalować aplikację Microsoftu na smartfonie z Androidem, postępujemy identycznie jak w przypadku aplikacji natywnych. Programy znajdziemy w Google Play. By skorzystać z funkcji oferowanych przez te aplikacje, konieczne może być założenie konta Microsoft. Najlepiej, by było to to samo konto, z którego korzystamy na naszym komputerze.

kż

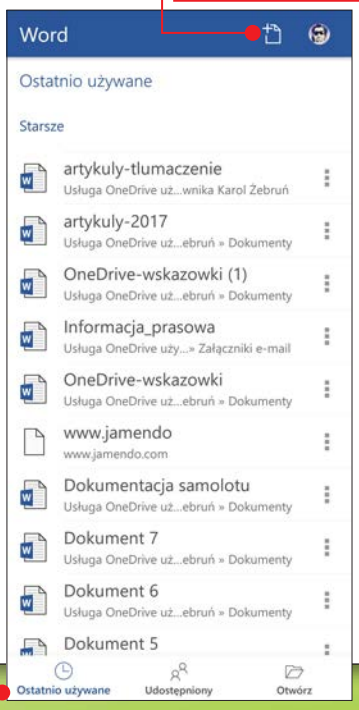
KORZYSTANIE Z APLIKACJI OFFICE

Prześledźmy instalację i rozpoczęcie pracy na przykładzie aplikacji Microsoft Word.



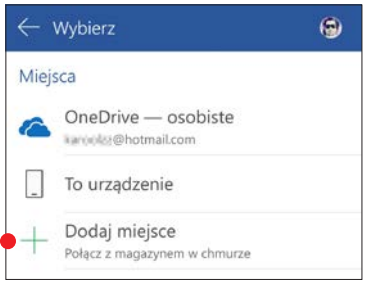
1 Instalujemy **Microsoft Word** z Google Play jak każdą inną aplikację na Androida. Po pierwszym uruchomieniu proszeni jesteśmy o zalogowanie się do konta Microsoft. Wpisujemy nazwę użytkownika i przechodzimy do kolejnego okna. (Jeśli chcemy korzystać z aplikacji lokalnie, wybieramy **Zaloguj się później**).

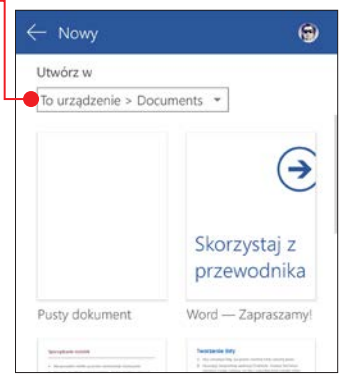
2 Wprowadzamy hasło i wybieramy **Zaloguj**. Otworzy się okno programu, w którym widzimy listę plików edytowanych wcześniej oraz udostępnionych. Możemy też otwierać pliki, wskazując je w pamięci urządzenia lub w chmurze.



3 By utworzyć nowy plik, wybieramy . Następnie dotykamy , by określić miejsce, gdzie będzie przechowywany. Domyślnie dokument zapisywany jest w pamięci smartfona. Jeśli chcemy zapisać go w chmurze, dotykamy **Wybierz inną lokalizację**.

4 Domyślnie możemy zapisać plik w jednym z folderów OneDrive'a, który jest połączony z naszym kontem (możemy też wskazać lokalizację inną niż chmura).



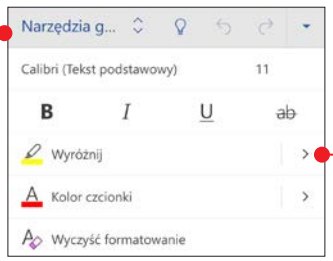


Wskazujemy folder docelowy i dotykamy **Wybierz**.

5 Teraz, dotykając, wybieramy szablon dla edytowanego pliku. Jeśli chcemy samodzielnie wpisywać treść, naciskamy **Pusty dokument**.

6 Edytowany plik jest automatycznie zapisywany we wskazanej lokalizacji sieciowej. Gdy brak połączenia z siecią, Word zachowa go tymczasowo w smartfonie.

7 By uzyskać dostęp do narzędzi edycyjnych, naciskamy ponad wirtualną klawiaturą. Narzędzia podzielone są na grupy, które wyświetlamy, dotykając . Tekst wklejamy i zaznaczamy podobnie jak w innych narzędziach dla Androida.



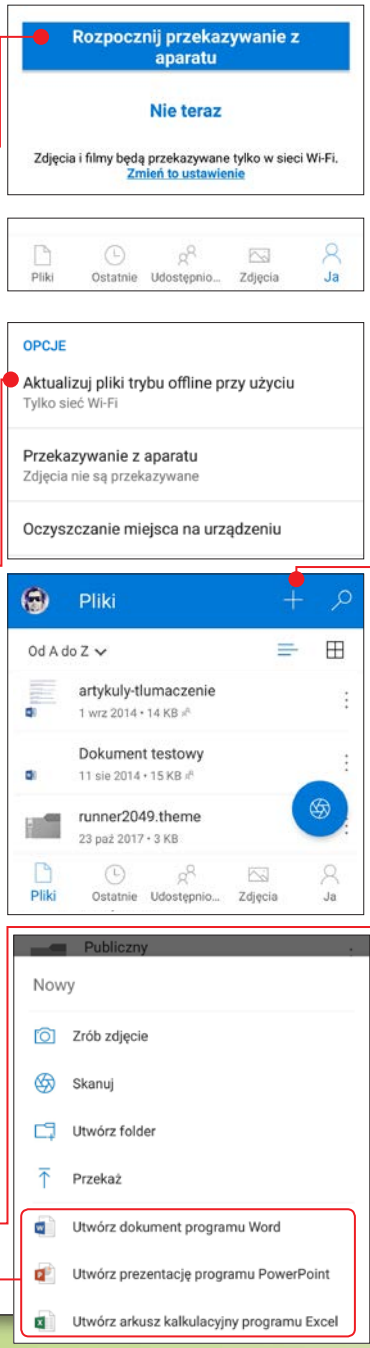
PRACA Z MICROSOFT ONEDRIVE

1 Po zainstalowaniu i zalogowaniu się do **OneDrive'a** przy pierwszym uruchomieniu będziemy poproszeni o włączenie funkcji ●. Jej zadaniem jest zapisywanie na bieżąco w chmurze Microsoft kopii zdjęć i filmów wykonanych smartfonem. Możemy zrezygnować z tej opcji, wybierając **Nie Teraz**.

2 By włączyć przesyłanie zdjęć, na zakładce **Ja** wybieramy **Ustawienia**, a potem **Przekazywanie z aparatu** i aktywujemy suwak narzędzia. Opcja ● pozwala wymusić aktualizację zawartości offline również przy użyciu sieci komórkowej.

3 Główne okno OneDrive'a pełni rolę menedżera plików. Po otworzeniu wybranego pliku na zakładce **Pliki** możemy go zapisać w pamięci smartfona albo rozpocząć edycję w aplikacji przypisanej do danego dokumentu. Z kolei zakładka **Zdjęcia** zawiera posortowane obrazy.

4 OneDrive umożliwia też stworzenie nowego dokumentu, na przykład pliku Excela. W tym celu klikamy na **Pliki**, na ●, a potem wybieramy jedną z opcji ●.



APLIKACJE MICROSOFT DLA ANDROIDA

Narzędzia Office – Word, Outlook, PowerPoint, Excel, OneNote

Uproszczone wersje sztandarowych narzędzi pakietu Office 365, które dzięki chmurze umożliwiają współdzielenie ze smartfonem środowiska pracy i tworzonych na pececie dokumentów. Gdy nie mamy dostępu do chmury, możemy wykorzystać programy jako czytniki i edytory dokumentów w formatach Office.

Microsoft Launcher

Narzędzie do personalizacji smartfona za pomocą motywów i integracji z usługami Microsoft. Pozwala tworzyć listę informacji, powiadomień, kontaktów Microsoft, która będzie pełnić rolę ekranu domowego smartfona. Umożliwia kontynuację pracy na komputerze.

Microsoft To-Do

Lista zadań do wykonania, której zawartość synchronizuje się z narzędziem pocztowym w Microsoft Outlook lub na witrynie Outlook.com.

Microsoft Remote Desktop

Narzędzie do klonowania zawartości pulpitu na komputerze do smartfona z Androidem. Pozwala wykorzystać ekran smartfona jako wirtualny pulpit dla aplikacji uruchomionych na komputerze.

Microsoft OneDrive

Aplikacja dostępowa do chmury OneDrive z funkcjami podglądu plików. Zapewnia łatwą synchronizację zawartości chmury ze smartfonem. Dostęp do aplikacji można blokować odciskiem palca.

Microsoft Authenticator

Ułatwia logowanie się do usług bez użycia hasła. Wykorzystuje naszą odpowiedź na powiadomienie przesłane na smartfon. Możemy też wykorzystać mechanizmy biometryczne smartfona dla zwiększenia bezpieczeństwa w procesie dwuetapowej autentyfikacji.

Microsoft Xbox

Aplikacja zapewniająca kontakt ze społecznością Xboxa. Działa jako agregator danych na temat naszych osiągnięć w grach. Umożliwia sterowanie konsolą Xbox One i zakupy w aplikacji.

Microsoft Office Lens

Zamienia aparat naszego smartfona w kieszonkowy skaner. Za jej pomocą wystarczy wykonać zdjęcie strony książki, tablicy, rachunku sklepowego lub innego dokumentu, by go zdigitalizować. Nie musimy nawet dokładnie umieszczać skanowanego/fotografowanego elementu w kadrze. Aplikacja automatycznie prostuje obraz, usuwa niepotrzebne elementy kadru, poprawia jego oświetlenie i próbuje dokonać rozpoznania tekstu. Możliwy jest zapis dokumentów w postaci plików Worda, PowerPointa, a także eksport do formatu PDF.

Microsoft Translator

Alternatywa dla narzędzi Google, która wykorzystuje silnik tłumaczący, wspierający 60 języków. Program może działać jako słownik z funkcjami poradnika wymowy, ale może też na żywo tłumaczyć napisy ze zdjęć i umożliwia dyskusję w dwu językach na podzielonym ekranie.

Microsoft Edge

Przeznaczona na smartfony wersja przeglądarki Microsoftu. Wspiera funkcje synchronizacji zawartości przeglądania, haseł, zakładek pomiędzy smartfonem a komputerem.

Pomocnik aplikacji Twój telefon

Narzędzie wspierające łączenie pracy na komputerze z Windows 10 i smartfonie z systemem Android.

Fot. Scanrail/123rf.com

ANONIMOWE SYS

*Na płycie dołączonej do tego wydania znajdziemy **pakiet trzech najlepszych anonimowych systemów** operacyjnych, które zapewniają prywatność lepiej niż Windows*

TAILS

Tails (DVD-KOD: **057**) jest to dystrybucja systemu Linux oparta na Debianie. Rozwinięcie skrótowca **T**he **A**mnesiac **I**ncognito **L**ive **S**ystem wskazuje, że jest to wersja **Live**. A to oznacza, że możemy z niej korzystać bez instalacji, bo do uruchomienia wystarczy dowolny nośnik (musimy go przygotować za pomocą programu **Rufus** DVD-KOD: **052**, również dostępnego na płycie). Uruchamiając system na przykład z pendrive'a, możemy pracować, nie zostawiając żadnych śladów w komputerze.

Do czego służy Tails

Głównym zadaniem tego systemu jest zapewnienie użytkownikowi jak największej anonimowości, prywatności i bezpieczeństwa w sieci. Jest to trudne – praktycznie cały ruch w internecie jest przecież rejestrowany. Dlatego Tails wymusza wszystkie połączenia z siecią przez **Tor**. Jeśli jakiś program chce uzyskać niechroniony dostęp, jest blokowany, aby nas nie zdekonspirował.

W systemie jest też wiele narzędzi, które zwiększają bezpieczeństwo – na przykład specjalne wtyczki do przeglądarki, które wymuszają szyfrowane połączenia.

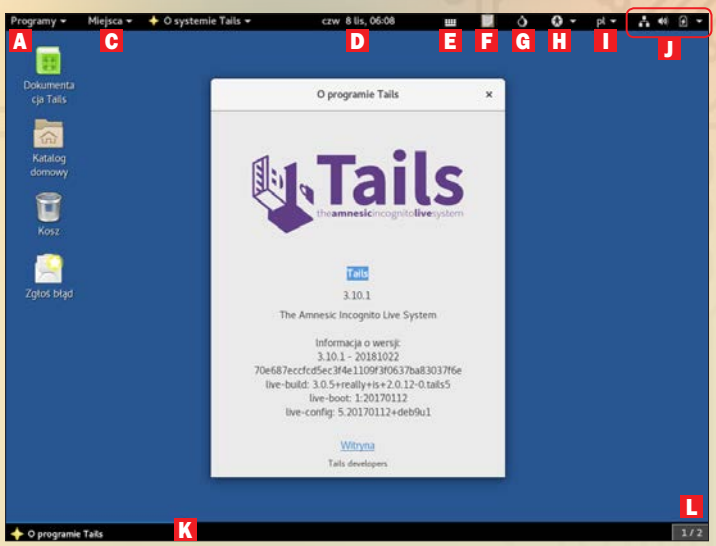
Pierwsze uruchomienie

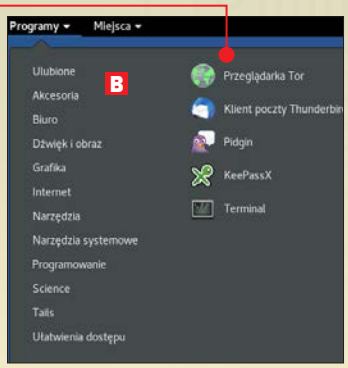
Po uruchomieniu systemu z bootowalnego nośnika pojawi się ekran powitalny. Wybieramy język systemu i typ klawiatury (domyślny jest angielski). Potem wystarczy kliknąć na **Uruchom Tails** (Start Tails).

Obsługa systemu

Interfejs systemu jest łatwy w obsłudze. Osoby korzystające na co dzień z Windows nie powinny mieć problemów. Oto gdzie co znajdziemy:

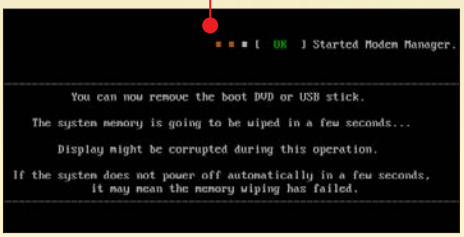
- **Programy** A – tu znajdziemy listę B z wszystkimi aplikacjami podzielonymi na kategorie; w kategorii **Ulubione** umieszczono bezpieczną anonimową przeglądarkę – **Tor**.
- **Miejsca** C – dostęp do najważniejszych katalogów w systemie
- **Kalendarz z zegarem** D
- **Wirtualna klawiatura** E – warto z niej korzystać przy logowaniu do ważnych witryn
- **OpenPGP Applet** F – pozwala zarządzać kluczami i szyfrować
- **Open Onion Circuit** G – informacje o dostępnych węzłach sieci
- **Ułatwienia dostępu** H
- **Wybór języka i klawiatury** I
- **Połączenia sieciowe**, **dźwięk** i **wyłączanie systemu** J
- **Pasek zadań** K z aktywnymi programami
- **Wybieranie obszarów roboczych** L





Jeśli przesuniemy kursor w skrajny lewy róg ekranu, otworzy się specjalny launcher znany z systemu Debian, który ułatwia znajdowanie programów i udostępnia wyszukiwarkę. Daje też podgląd aktywnych okien na każdym obszarze roboczym.

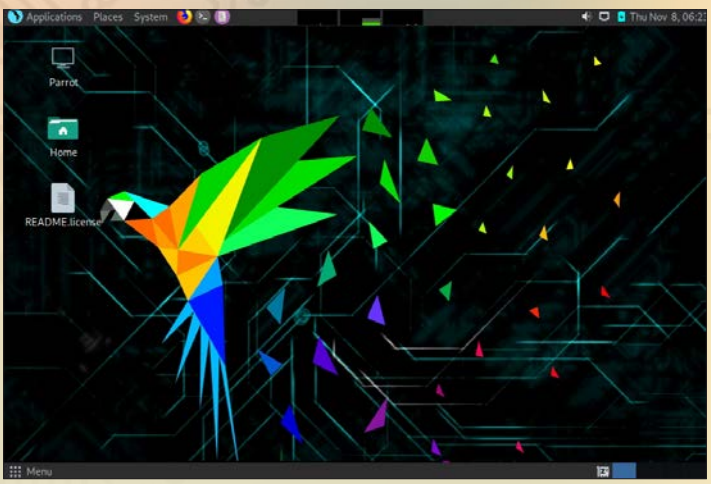
Kiedy wyłączamy system, Tails zawsze stara się zatrzeć wszelkie ślady korzystania z komputera, w tym celu wykonywane jest czyszczenie pamięci RAM. Informacja o tym pojawia się przez kilka sekund na ekranie.



KOMPLEKSOWY PORADNIK DOTYCZĄCY KORZYSTANIA Z TAILSA ZNAJDZIEMY W KSIĄŻCE Z SERII **BIBLIOTECZKA KOMPUTER ŚWIATA 1/2018** DOSTĘPNEJ W KS+ **WWW.KSPLUS.PL**

TEMY OPERACYJNE

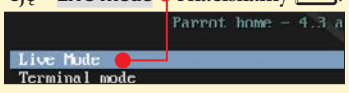
PARROT HOME



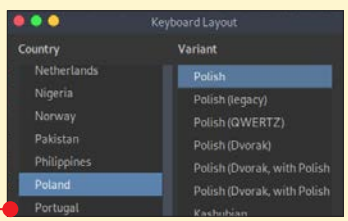
Parrot Home (DVD-KOD: **042**) dba o zachowanie anonimowości i prywatności użytkownika i daje dostęp do wielu narzędzi diagnostycznych i testowych, między innymi dla środowiska sieciowego. Występuje w wielu wersjach – mniej i bardziej rozbudowanych. Wersja **Home**, którą znajdziemy na płycie, to lekki Linux, który płynnie działa nawet na słabszych maszynach. Znajdziemy w nim programy między innymi do bezpiecznej komunikacji ze znajomymi i szyfrowania dokumentów. Warta uwagi jest też wersja **Security**, przeznaczona dla zaawansowanych użytkowników. Zawiera najważniejsze narzędzia do testów penetracyjnych sieci i systemów operacyjnych.

Korzystamy z systemu

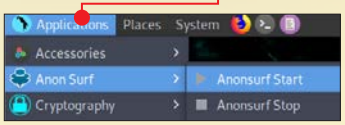
Po uruchomieniu komputera z bootowalnego nośnika z systemem (trzeba go przygotować za pomocą programu **Rufus** DVD-KOD: **052**, dostępnego na płycie) pojawi się Boot Menu. Za pomocą klawiszy strzałek wskazujemy w nim pierwszą pozycję – **Live Mode** i naciskamy enter.



Gdy pojawi się pulpit systemu, zostaniemy zapytani o układ klawiatury – wskazujemy po lewej stronie **Poland**, a po prawej **Polish**.



W systemie znajdziemy dwie przeglądarki – **Mozilla Firefox**, która ma wbudowane specjalne dodatki zwiększające anonimowość i bezpieczeństwo, i **Tor**, zapewniającą całkowitą anonimowość. Sieć TOR nie zawsze jest najlepszym rozwiązaniem, na przykład jeśli chcemy oglądać filmy w serwisie YouTube, możemy swobodnie korzystać ze zwykłej przeglądarki, a nie sieci TOR, która działa znacznie wolniej i służy do bardziej anonimowych zadań. Jeśli chcemy całkowitej anonimowości, klikamy w górnym lewym rogu pulpitu na **Applications**, **Anon Surf**,



Anonsurf Start. Aktywujemy w ten sposób specjalny tryb, który nie pozwoli żadnej aplikacji w tle zdradzić naszej tożsamości i lokalizacji. Cały ruch sieciowy jest kierowany przez bezpieczne kanały. Po zakończeniu anonimowej sesji wystarczy wybrać z menu **Anonsurf Stop**.

KALI LINUX

Kali Linux (DVD-KOD: **022**) to wyjątkowy system, który zawiera dużo narzędzi od razu gotowych do pracy i przeznaczonych dla zaawansowanych użytkowników. Właściwe ich wykorzystanie wymaga sporej praktyki i doświadczenia, ale nawet początkujący będą w stanie posłużyć się kilkoma podstawowymi. Nieco więcej na ten temat przeczytamy na stronie 72.

Uwaga! Domyślny użytkownik w wersji Live to **root**, a hasło to **toor**.

ABC Kali Linuxa

Domyślnie nie można umieszczać skrótów do programów na pulpicie, ponieważ nakładką graficzną w systemie Kali jest **Gnome**.

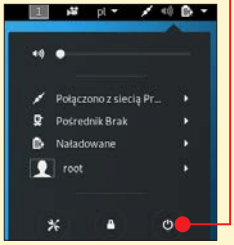
Po lewej stronie ekranu jest pasek szybkiego dostępu **A**, na którym znajdują się programy z kategorii **Ulubione**. Po kliknięciu prawym przyciskiem myszy na aplikację możemy ją usunąć z tej kategorii. Dodawanie do Ulubionych wygląda podobnie – wystarczy prawym przyciskiem myszy kliknąć na ikonę aplikacji i wybrać opcję **Dodaj do ulubionych**.

Na samym dole paska szybkiego dostępu widać przycisk **B**, który pozwala na wyświetlenie prawie wszystkich programów zainstalowanych w systemie (**Wszystkie**).

Niektóre narzędzia są dostępne tylko po wpisaniu odpowiedniej komendy w terminalu.

Górny pasek możemy traktować jak pasek zadań w systemie Windows. Po kliknięciu na **Programy** otworzy się menu z wszystkimi aplikacjami podzielonymi na odpowiednie kategorie. Po kliknięciu na **Miejsca** będziemy mogli szybko dostać się do najważniejszych folderów w systemie i na dysku.

System zamykamy, klikając na strzałkę w górnym prawym rogu, a następnie na symbol wyłączania. **kd**



Fot. iterum/123rf.com

TRIKI
DO INTERNETU
OTWARTE WI-FI A BEZPIECZEŃSTWO

BEZPIECZNE KORZYSTANIE Z OTWARTEGO WI-FI

Z darmowego dostępu do internetu za pośrednictwem otwartych hotspotów korzystamy w restauracjach, centrach handlowych, na lotniskach. ***Należy jednak uważać****, ponieważ takich sieci mogą używać również hakerzy, którzy chcą zdobyć nasze dane*

Jeśli często korzystamy z publicznych sieci Wi-Fi, powinniśmy poznać podstawowe zasady bezpieczeństwa, które mogą oszczędzić nam kłopotów i nerwów. Warto też znać możliwości, jakie daje hakerom otwarta sieć Wi-Fi.

Jeden z najtrudniejszych elementów ataku na dowolną osobę to przechwycenie jej ruchu sieciowego. Jeśli haker nie znajduje się w tej samej sieci LAN lub WLAN co potencjalna ofiara, jest to bardzo skomplikowane. A w wypadku otwartych sieci – to łatwe. Dlatego też publiczne Wi-Fi jest jak zaproszenie dla hakera. Bez problemu może połączyć się z siecią, z której korzysta wiele osób, i przejść do przygotowania ataku na użytkowników, którzy są aktualnie aktywni.

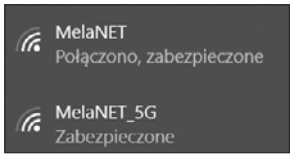
Dość często zdarza się też, że hakerzy umieszczają swoje rutery w publicznych miejscach i udostępniają darmowy hotspot, z którego chętnie korzysta wielu użytkowników nieświadomych, że cały ruch sieciowy jest rejestrowany i może być wykorzystany przez atakującego do zdobycia ważnych haseł i loginów.

Niektóre z podanych obok zasad bezpieczeństwa warto zastosować również do smartfonów.

Więcej o tym, jak wyglądają ataki wewnątrz sieci, przeczytamy na stronie 72. **kd**

ZASADY BEZPIECZNEGO KORZYSTANIA Z OTWARTYCH SIECI

1 SPRAWDZAMY, CZY ŁĄCZYMY SIĘ Z ODPOWIEDNIĄ SIECIĄ



Jeśli zamierzamy skorzystać z darmowego hotspota, sprawdźmy, czy na pewno łączymy się z odpowiednim punktem, a nie siecią, która tylko udaje nasz punkt. Najprościej jest zapytać obsługę hotelu, restauracji czy też innego obiektu udostępniającego sieć o poprawną nazwę sieci. Często różnica może być niewielka – na przykład jeden inny znak w SSID, czyli identyfikatorze sieci.

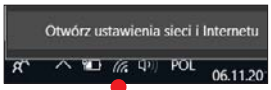
2 AUTOMATYCZNE ŁĄCZENIE SIĘ Z SIECIĄ

Jest to jedna z bardziej przydatnych opcji dostępna na takich urządzeniach, jak laptopy czy smartfony. Wracamy do domu lub przychodzimy do pracy i nasze urządzenia automatycznie łączą się z siecią. Należy jednak uważać, jakie sieci mamy dodane do opcji automatycznego łączenia. Jeśli często odwiedzamy fast food, który w każdym swoim punkcie udostępnia sieć o tej samej nazwie, możemy być narażeni na atak osoby, która stworzy hotspot o tej nazwie i tym samym urządzenia będą łączyły się bez naszej wiedzy z niewłaściwą siecią. Dlatego też warto wyłączyć opcję automatycznego łączenia dla sieci publicznych.

3 WYŁĄCZAMY UDOSTĘPNIANIE PLIKÓW

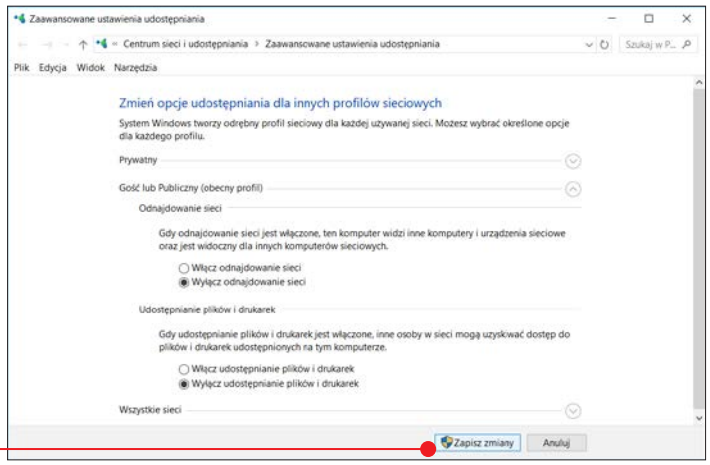
Jeśli połączymy się z siecią otwartą i wybierzemy odpowiedni profil sieci, nie oznacza to, że nasze dane nie będą udostępniane. Musimy sami o to zadbać, sprawdzając poprawność ustawień systemowych profili sieciowych.

1 Klikamy prawym przyciskiem myszy na ikonę sieci w zasobniku systemowym, a następnie na **Otwórz ustawienia sieci i Internetu**.



2 Teraz po prawej stronie klikamy na **Opcje udostępniania**.

3 Następnie dla profilu **Gość** zaznaczamy opcję wyłączenia udostępniania i klikamy na **Zapisz zmiany**.

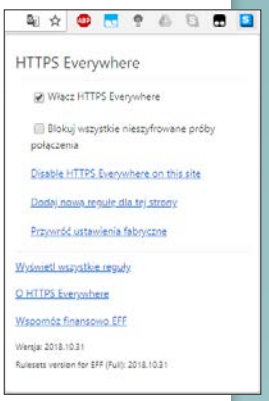


6 PODWÓJNE UWIERZYTELNIANIE DLA DODATKOWEJ OCHRONY

Jeśli przez przypadek nasze hasło wpadnie w niepowołane ręce, a my wcześniej skonfigurujemy opcję logowania dwuetapowego, nasze konta będą dalej bezpieczne. Podwójne uwierzytelnienie polega na zalogowaniu w dwóch etapach – pierwszy to wykorzystanie zwykłego hasła w panelu logowania, drugi natomiast to na przykład dodatkowy kod, który przyjdzie jako SMS lub e-mail. Więcej o podwójnym uwierzytelnianiu przeczytamy na stronie 94.

7 KORZYSTAMY Z HTTPS

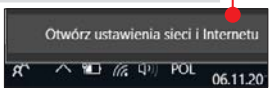
Jeśli zamierzamy korzystać z internetu poprzez otwarte sieci, warto dodatkowo się zabezpieczyć. Jednym z takich zabezpieczeń jest zwracanie uwagi na pasek przeglądarki i na to, czy po prawej stronie znajduje się symbol kłódki, a adres strony rozpoczyna się od **HTTPS**. Jeśli tak jest, możemy być pewni, że pakiety sieciowe, które nasze urządzenie generuje oraz odbiera z serwerów zewnętrznych, są odpowiednio szyfrowane i zabezpieczone. Pakiety HTTP można bardzo łatwo odczytać i wykraść z nich dane dotyczące choćby logowania. Nie wszystkie witryny oferują taką formę przeglądania automatycznie, dlatego też warto skorzystać z pluginu dostępnego dla wszystkich popularnych przeglądarek – **HTTPS Everywhere**. Po dodaniu tego dodatku do naszej przeglądarki będzie on automatycznie wymuszał nawiązywanie połączenia ze wszystkimi stronami w standardzie HTTPS, jeśli to tylko możliwe.



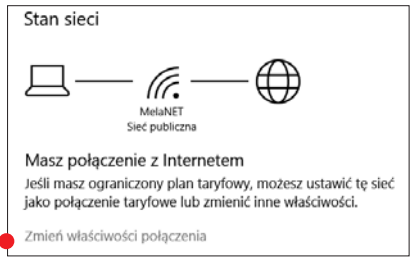
4 ZMIANA PROFILU SIECI

Jeśli łączymy się z otwartą siecią poprzez urządzenie z Windows, warto wiedzieć, że system zapyta nas przy nawiązaniu połączenia o to, jak ma traktować daną sieć – jako publiczną czy domową. Wiele osób przez przypadek może wybrać drugą opcję, a wtedy nasze pliki (filmy, muzyka, obrazy, dokumenty) zostaną udostępnione dla wszystkich użytkowników danej sieci. Jest to bardzo niebezpieczne i należy upewnić się, czy mamy aktywny odpowiedni profil dla sieci otwartej.

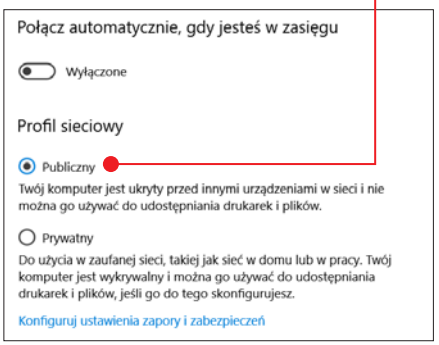
1 Klikamy prawym przyciskiem myszy na ikonę sieci w zasobniku systemowym, a następnie na **Otwórz ustawienia sieci i Internetu**.



2 Następnie po prawej stronie klikamy na opcję **Zmień właściwości połączenia**.



3 Teraz wystarczy wybrać opcję **Publiczny** i wyjść z okna ustawień.



5 KORZYSTAMY Z FIREWALLA I PROGRAMU ANTYWIRUSOWEGO

To „podstawa podstaw", a jednak wciąż zdarzają się użytkownicy przeglądający zasoby internetu bez żadnej ochrony. Wystarczy jedno wejście na nieodpowiednią stronę lub pobranie i uruchomienie nieodpowiedniego pliku, a nasz komputer zostanie zainfekowany złośliwymi programami.
Zabezpieczenie jest szczególnie ważne, gdy korzystamy z otwartych sieci, ponieważ jeśli mamy nieaktualny system operacyjny i nie mamy żadnej dodatkowej osłony, atakujący może wykorzystać to i włamać się do naszego urządzenia. Gdyby w tle aktywny był firewall i antywirus, atak zostałby powstrzymany.

POLECAMY ANTYWIRUSY:
BITDEFENDER – DOSTĘPNY Z PRENUMERATĄ KOMPUTER ŚWIATA, G DATA IS – NA ROK ZA DARMO DLA STAŁYCH CZYTELNIKÓW KOMPUTER ŚWIATA, ESET INTERNET SECURITY – NA ROK ZA DARMO DLA STAŁYCH CZYTELNIKÓW NIEZBĘDNIKA

8 KORZYSTAMY Z VPN

Jeśli chcemy być całkowicie bezpieczni w otwartej sieci, warto skorzystać z możliwości połączeń z siecią VPN. Umożliwi nam to korzystanie z otwartej sieci, a jednocześnie uniemożliwi hakerom przejęcie naszych pakietów sieciowych, które będą całkowicie zaszyfrowane. Więcej o takich sieciach przeczytamy na stronie 84, a najlepsze programy znajdziemy na stronie 88.

Fot. Happymay/123rf.com

USTAW SWÓJ RUTER

Centralnym punktem domowej sieci jest zwykle ruter Wi-Fi. Warto zadbać o jego poprawną konfigurację – dzięki temu nasza ***sieć będzie działać wydajniej i stabilniej****, będzie też bezpieczniejsza*

Popularność sieci bezprzewodowych w naszych domach wynika wprost z wygody użytkowania tego rozwiązania. Kupujemy ruter, podłączamy kabel lub modem od operatora internetowego i gotowe. Nie ma przy tym znaczenia, czy internet mamy z Orange (dawna Neostrada), czy łącze z kablówki, czy też od innego operatora, na przykład komórkowego z dostępem przez LTE. Wielu producentów maksymalnie upraszcza procedurę wstępnej konfiguracji rutera, głównie dlatego, by nabywca urządzenia jak najszybciej mógł cieszyć się ze swojej nowej, domowej sieci bezprzewodowej. Szybko nie zawsze znaczy jednak dobrze. Dlatego warto trochę w ustawieniach rutera podłubać. **as**

KONFIGUROWANIE RUTERA – ZASADY OGÓLNE

Zanim przejdziemy do przykładów pokazujących konfigurację ruterów popularnych w Polsce marek, warto poznać kilka ogólnych zasad.

1 Potrzebujesz tylko przeglądarki

Ustawianie parametrów pracy i konfigurowanie różnych funkcji rutera sieci bezprzewodowej odbywa się najczęściej za pośrednictwem specjalnego adresu IP, przekierowującego do strony z panelem administracyjnym danego rutera. Ten panel administracyjny to nic innego jak strona internetowa, której wszystkie zasoby znajdują się w pamięci wewnętrznej rutera. Oznacza to, że aby móc konfigurować ruter we własnej sieci, potrzebujemy do tego dowolnego znajdującego się w niej komputera i dowolnej przeglądarki WWW. Żadne dodatkowe oprogramowanie nie jest potrzebne.

2 Zmień ustawienia fabryczne

Każdy ruter jest prekonfigurowany fabrycznie. Producent ustawia w nim domyślne parametry pracy, dotyczy to również fabrycznego loginu administracyjnego i hasła. Problem w tym, że fabryczne loginy i hasła są powszechnie znane. Jeżeli ich nie zmienimy, każdy odpowiednio zdeterminowany haker (czy choćby złośliwy sąsiad posiadający odpowiednią wiedzę – wcale nie za dużą) będzie mógł przejąć kontrolę nad ruterem po złamaniu zabezpieczeń sieci Wi-Fi.

3 Dbaj o aktualizacje oprogramowania rutera

Ruter, jak każdy inny sprzęt, działa, opierając się na oprogramowaniu wewnętrznym. Oprogramowanie to, jak każde, może zawierać luki. Niezaktualizowany ruter to zaproszenie dla hakerów. Dlatego warto co jakiś czas logować się do panelu administracyjnego rutera i sprawdzać, czy jego producent nie udostępnił aktualizacji firmware'u.

4 Nie udostępniaj danych logowania do sieci osobom postronnym

Domowa sieć Wi-Fi powinna służyć tylko domownikom. A jeżeli przyjdą znajomi i będą chcieli uzyskać dostęp do naszej sieci, warto ustawić w ruterze niezależną sieć dla gości, a nie podawać identyfikator i hasło dostępowe do naszej sieci głównej.

Wiele współczesnych ruterów oferuje możliwość utworzenia drugiej sieci gościnnej o innym poziomie zabezpieczeń. Sposób ustawiania takiej sieci został opisany na stronie 66.

5 Wykorzystaj potencjał posiadanego urządzenia

Funkcje współczesnych ruterów znacznie wykraczają poza zwykłe udostępnianie łącza internetowego. Obecnie domowy ruter Wi-Fi można wykorzystać również jako sieciową pamięć masową (po podłączeniu do niego na przykład dysku USB) czy serwer druku. W dalszej części poradnika przeczytamy, jak zmienić ruter w serwer multimedialny.

Ponieważ różni producenci oferują różnie wyglądające panele administracyjne ruterów, we wskazówkach na kolejnych stronach przedstawiono panele różnych producentów. Nie znaczy to oczywiście, że daną funkcję można zrealizować wyłącznie w prezentowanym urządzeniu konkretnej marki, większość ruterów dysponuje wszystkimi pokazywanymi tu ustawieniami.

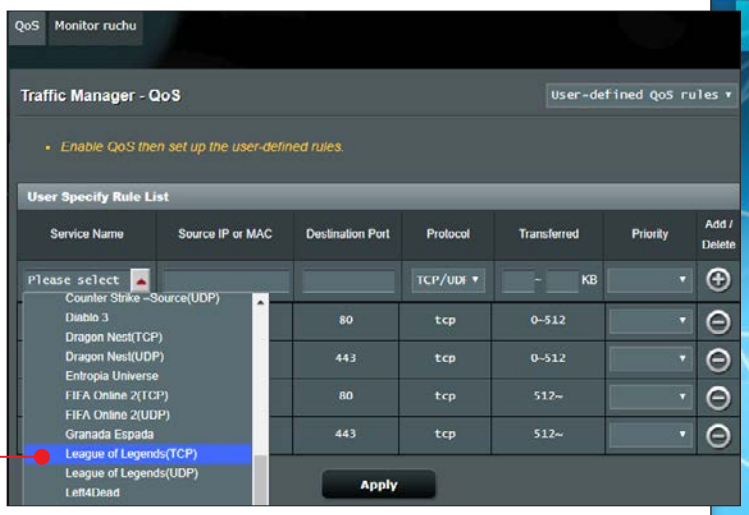
USTAWIENIA DOMOWEJ SIECI WI-FI NA PRZYKŁADZIE PANELU ADMINISTRACYJNEGO RUTERA ASUS

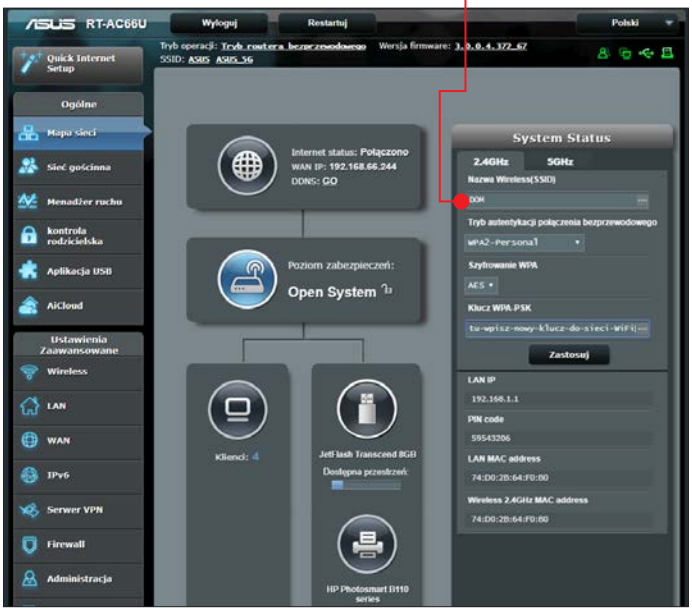
W nowoczesnym ruterze mamy do dyspozycji wiele przydatnych funkcji, które mają wpływ na jakość, stabilność i wydajność domowej sieci bezprzewodowej. Poznajmy je na przykładzie panelu administracyjnego w ruterach ASUS. Dostęp do panelu uzyskujemy po wpisaniu w przeglądarce adresu IP: **192.168.1.1**. Zakładając, że dopiero konfigurujemy sieć bezprzewodową, należy komputer, z którego korzystamy, połączyć z ruterem kablem sieciowym.

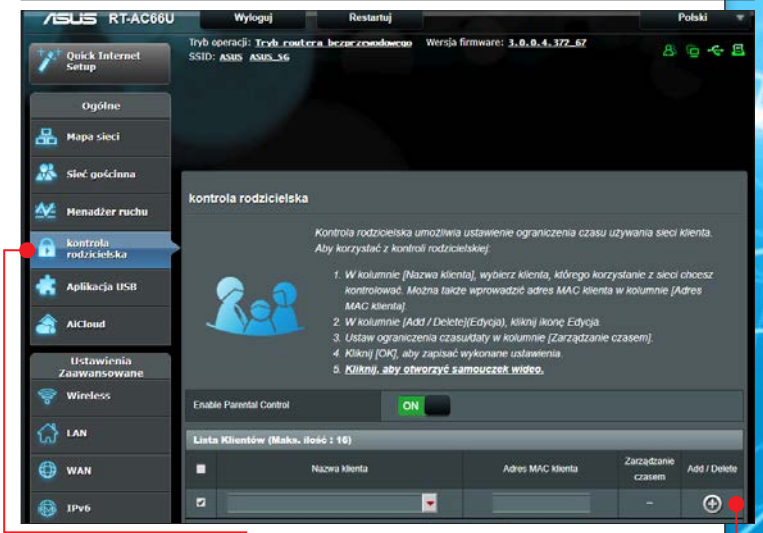
1 Po zalogowaniu się do panelu administracyjnego (hasło domyślne podawane jest w instrukcji obsługi rutera) widoczna jest mapa sieci. Zacznijmy od zdefiniowania dwóch sieci Wi-Fi działających w pasmach 2,4 GHz oraz 5 GHz. W sekcji **System status** na karcie **2.4GHz** wprowadzamy nazwę domowej sieci Wi-Fi, następnie z rozwijalnej listy wybieramy najsilniejsze obecnie dostępne szyfrowanie **WPA2-Personal** oraz **AES** i wprowadzamy klucz – hasło, które będzie chronić dostępu do naszej sieci. Czynności te powtarzamy dla drugiego pasma po przejściu na kartę **5GHz**.

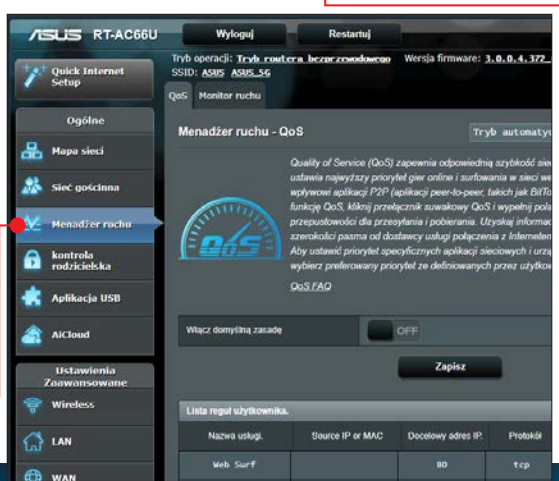
2 Jeżeli często gramy online, można tak skonfigurować ruter, by ruch związany z pakietami danej gry był traktowany priorytetowo. W nowoczesnych ruterach umożliwiają to ustawienia **QoS (Quality of Service)**. W przypadku ruterów ASUS znajdziemy je po wybraniu z menu po lewej stronie opcji **Menadżer ruchu**. Standardowo funkcje QoS działają w trybie automatycznym, w którym najczęściej najwyższy priorytet dostępu do wydajności łącza ma internetowa przeglądarka i protokół HTTPS.

3 Chcąc dodać regułę dla konkrentej gry online, na przykład League of Legends, należy przełączyć Menadżera ruchu z trybu automatycznego A i wybrać z listy rozwijalnej **Priorytet definiowany przez użytkownika**. Następnie z listy rozwijalnej w kolumnie **Service Name** wybieramy nazwę gry, której chcemy przyznać priorytetowy dostęp do łącza. A w kolumnie **Priority** ustawiamy najwyższy priorytet. Analogicznie możemy postąpić z innymi usługami. Oczywiście należy pamiętać, że przyznawanie najwyższego priorytetu wielu usługom nie ma sensu. Warto to robić jedynie dla niewielu wybranych aplikacji i usług.







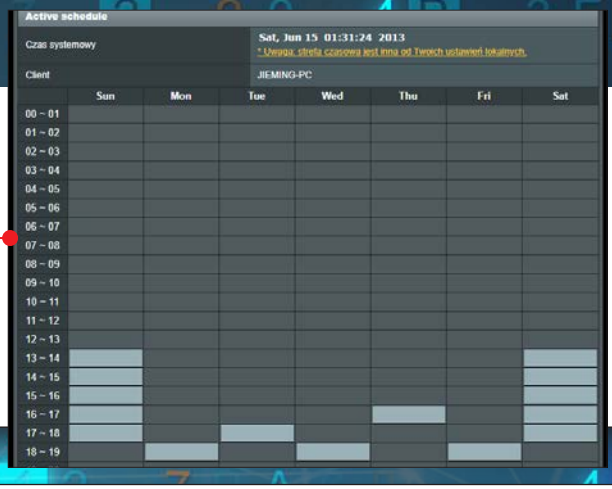


4 Rodzice, którzy obawiają się o to, że ich dzieci będą zbyt długo używać internetu, mogą skorzystać z oferowanej w oprogramowaniu ruterów funkcji kontroli rodzicielskiej. W ruterach ASUS odpowiednie funkcje znajdziemy po kliknięciu w menu na przycisk **Kontrola rodzicielska**.

5 Po wywołaniu panelu kontroli rodzicielskiej aktywujemy przełącznik **Enable Parental Control**, a następnie z listy **Nazwa klienta** wybieramy urządzenie, które chcemy kontrolować (czyli komputer lub smartfon dziecka), a potem klikamy na symbol w kolumnie **Add/Delete**. Gdy w tabeli pojawi się

dodana pozycja, klikamy na kolumnę **Zarządzanie czasem**.

6 Po kliknięciu zobaczymy tabelę z przedziałami godzin i dni tygodnia. Klikając na odpowiednie pola, definiujemy, kiedy dane urządzenie (komputer lub smartfon dziecka) będzie miało dostęp do sieci.

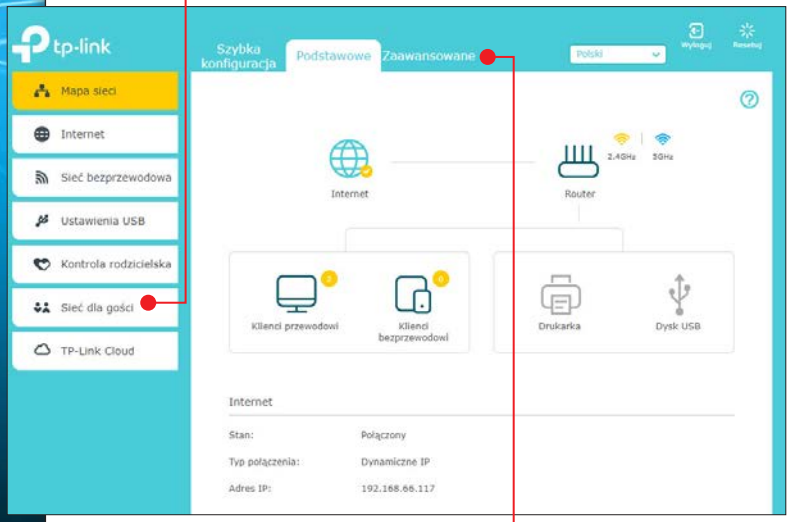


SIEĆ DLA GOŚCI I SPRAWDZENIE AKTUALIZACJI NA PRZYKŁADZIE RUTERA TP-LINK

Jeżeli odwiedzają nas znajomi, którzy potrzebują skorzystać z dostępu do internetu, podawanie im hasła dostępowego do głównej, domowej sieci Wi-Fi jest złym pomysłem. We współczesnych ruterach istnieje rozwiązanie tego problemu – możliwość utworzenia niezależnej sieci Wi-Fi dla gości. Oto jak tego dokonać za pomocą panelu konfiguracyjnego ruterów TP-Link na przykładzie modelu **TP-Link Archer C7**. A w drugiej części wskazówki przeczytamy, jak aktualizować oprogramowanie rutera

Ustawianie sieci dla gości

1 Panel konfiguracyjny ruterów TP-Link wygląda zupełnie inaczej od wcześniej wymienionego ASUSA, ale to głównie kwestia estetyczna, gdyż opcje w oprogramowaniu każdego rutera są podobne. Również dostęp uzyskujemy podobnie – wpisując adres IP rutera w pasku adresowym przeglądarki internetowej. W przypadku ruterów TP-Link funkcja konfigurowania gościnnej sieci Wi-Fi znajduje się w bocznym menu panelu administracyjnego jako jedna z głównych opcji tego menu. Aby ustawić sieć dla gości, klikamy na ten właśnie element.

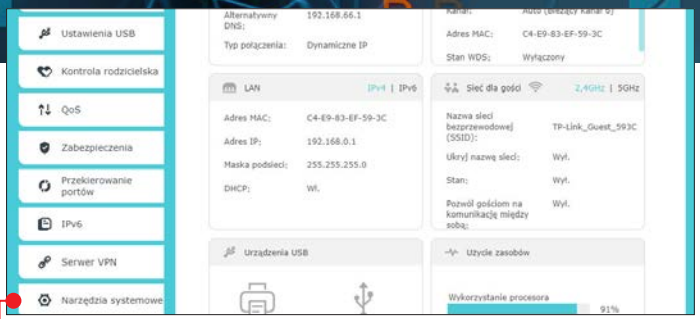


2 Po wybraniu z bocznego menu **Sieć dla gości** w centralnej części panelu zobaczymy opcje konfiguracyjne gościnnego Wi-Fi. Jeżeli goście potrzebują po prostu dostępu do internetu umożliwiającego zwykłe surfowanie po stronach WWW, nie ma potrzeby aktywowania pól wyboru **Pozwól gościom na komunikację między sobą**, a tym bardziej nie należy uaktywniać pola **Pozwól gościom na dostęp do sieci lokalnej**.

3 W naszym przykładzie ruter TP-Link Archer C7 komunikuje się w dwóch zakresach radiowych sieci Wi-Fi: w paśmie 2,4 GHz oraz w paśmie 5 GHz. Za pomocą panelu administracyjnego rutera możemy utworzyć dwie sieci Wi-Fi dla gości, z których każda będzie działać w odrębnym z tych dwóch pasm. Nazwę (identyfikator SSID) pierwszej gościnnej sieci działającej w paśmie 2,4 GHz wprowadzamy w pole **Nazwa sieci bezprzewodowej (SSID)**: widoczne pod napisem **Sieć bezprzewodowa 2,4 GHz**. Analogicznie postępujemy w przypadku sieci 5 GHz. Dla obu sieci ustawiamy hasło dostępowe, które musi być inne niż hasło do naszej głównej domowej sieci bezprzewodowej. Kliknięcie na przycisk **Zapisz** powoduje zapisanie zmian w konfiguracji rutera – od tej pory znajomi będą mogli skorzystać z internetu w naszym domu i jednocześnie nie uzyskają dostępu ani do naszej domowej sieci, ani do naszych prywatnych zasobów.

Sprawdzenie aktualizacji oprogramowania rutera

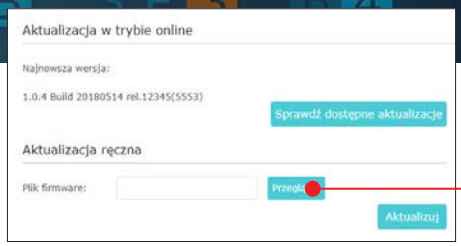
1 Aby uzyskać dostęp do ustawień związanych z aktualizacją oprogramowania ruterów TP-Link, należy najpierw w panelu administracyjnym aktywować ustawienia zaawansowane. Klikamy na kartę **Zaawansowane**. Domyślnie ruter wyświetli ekran **Stan**, na którym wyświetlone są aktualne parametry sieci, internetu i podłączonych urządzeń.



Aby przejść do opcji związanych z aktualizacją, należy w bocznym menu wybrać pozycję **Narzędzia systemowe**.

2 Po kliknięciu w menu na **Narzędzia systemowe** rozwinie się lista i zobaczymy pozycje. Jedną z nich jest element o nazwie **Aktualizacja firmware** – na niego właśnie powinniśmy kliknąć.

3 W oknie panelu administracyjnego rutera zobaczymy ekran z opcjami aktualizacyjnymi. W górnej części wyświetlane są informacje na temat aktualnie zainstalowanej wersji firmware'u. W sekcji **Aktualizacja w trybie online** widoczny jest przycisk **Sprawdź dostępne aktualizacje**. Gdy na niego klikniemy, ruter połączy się

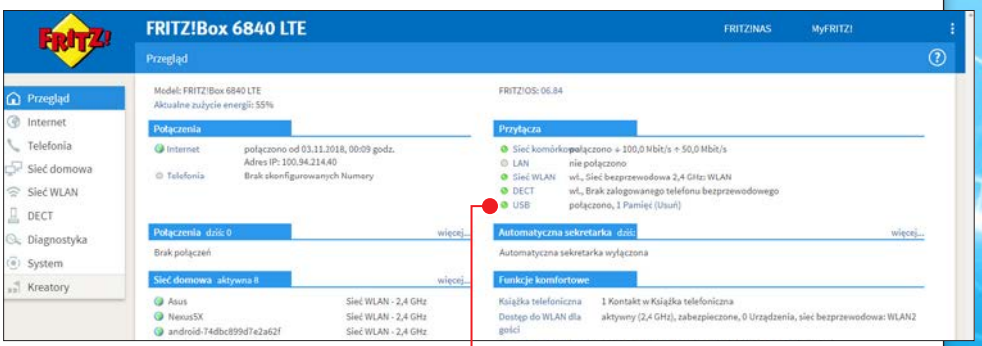


z serwerem aktualizacyjnym producenta. W przypadku wykrycia nowszej wersji oprogramowania możliwe będzie przeprowadzenie aktualizacji automatycznej. Oprócz tego istnieje jeszcze możliwość aktualizacji ręcznej. W tym celu należy wcześniej pobrać plik firmware'u właściwego dla konkretnego modelu rutera, a następnie w panelu konfiguracyjnym rutera wskazać ten plik (przycisk **Przeglądaj**). Po wskazaniu klikamy na przycisk **Aktualizuj**. **Uwaga!** Procesu aktualizacji firmware'u rutera nie można przerwać – może to grozić całkowitą utratą dostępu do rutera (konieczne będzie oddanie urządzenia do serwisu).

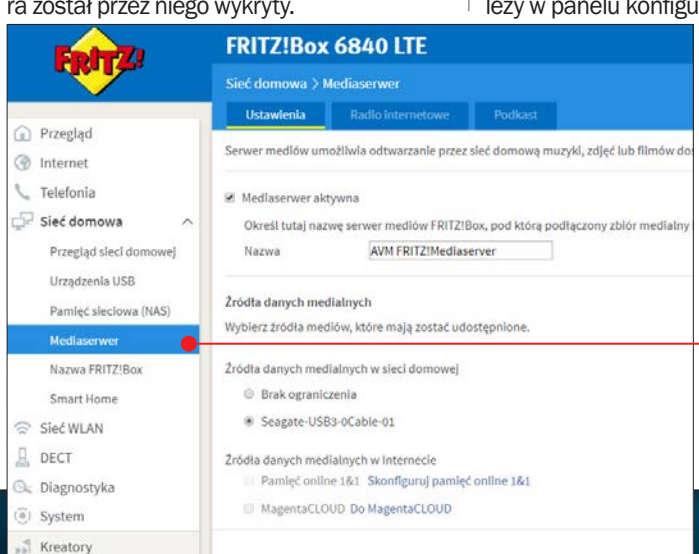
RUTER WI-FI JAKO SERWER MULTIMEDIALNY

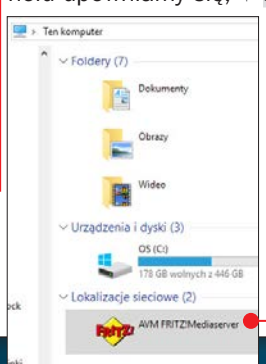
Większość obecnie dostępnych ruterów może również funkcjonować jako domowe serwery plików czy NAS-y (Network Attached Storage), czyli pamięć masowa dostępna przez sieć lokalną. Wystarczy, że do gniazda USB w ruterze podłączymy na przykład przenośny dysk twardy USB. Konfigurację funkcji NAS w ruterze poznamy na przykładzie rutera **AVM Fritz!Box 6840 LTE**.

1 Zaczynamy od podłączenia dysku USB do gniazda USB w ruterze. Następnie w przeglądarce internetowej wprowadzamy adres IP panelu administracyjnego rutera (w przypadku naszego rutera był to adres **192.168.178.1**). Już na głównym ekranie panelu administracyjnego systemu Fritz!OS (oprogramowanie wewnętrzne w ruterach AVM), w sekcji **Przyłącza** powinniśmy zobaczyć wpis **USB** i **połączono**, co oznacza, że dysk USB podłączony do rutera został przez niego wykryty.



2 Dostęp do zasobów zapisanych na dysku podłączonym do rutera możemy uzyskiwać na co najmniej dwa sposoby – poznajmy najprostszy. Standardowo w ruterach AVM jest funkcja mediaserwera – każdy podłączony do USB zasób pamięci (dysk) może być indeksowany przez ruter, a jego zawartość będzie dostępna poprzez mediaserwer. W tym celu należy w panelu konfiguracyjnym rutera przejść do menu **Sieć domowa** i podmenu **Mediaserwer**. Następnie po prawej stronie panelu upewniamy się, że zaznaczone jest pole wyboru **Mediaserwer aktywna**. W sekcji **Źródła danych medialnych w sieci domowej** sprawdzamy, czy zaznaczona jest opcja przy nazwie podłączonego dysku (w naszym przykładzie jest to Seagate-USB3-0Cable-01). Klikamy na **Zastosuj**.





3 Aby uzyskać dostęp do danych na dysku przez funkcję mediaserwera, wystarczy otworzyć okno Eksploratora na komputerze podłączonym do domowej sieci. W oknie **Ten komputer**, w sekcji **Lokalizacje sieciowe** powinniśmy zobaczyć element **AVM FRITZ!Mediaserver**. Przeglądanie zasobów w mediaserwerze wygląda inaczej niż w Eksploratorze. Mediaserwer indeksuje pliki według typów, po otwarciu jego okna zobaczymy foldery: **Filmy**, **Obrazy**, **Muzyka** itp. W tych folderach są pliki danego typu wykryte na podłączonym do rutera dysku, bez względu na to, w jakim folderze są na tym dysku zapisane. Udostępniony dysk będzie widoczny nie tylko dla każdego komputera w domowej sieci, ale też dla innych urządzeń, takich jak smart TV połączony z domową siecią, sprzęt audio z Wi-Fi itp.

Fot. Iuliia Kvasha, Nikita Gonin/123rf.com

ZABEZPIECZAMY

Jeśli mamy ruter zapewniający wielu urządzeniom w domu bezprzewodowy dostęp do internetu i domowej sieci, ***bardzo ważne jest zadbanie o bezpieczeństwo****. Nie chcemy przecież, aby ktoś włamał się do naszej sieci i wyrządził szkody*

Mało kto obecnie planuje w mieszkaniu sieć przewodową – znacznie prościej i wygodniej jest korzystać z sieci bezprzewodowej. Wydajność takiego rozwiązania na ogół jest zadowalająca. Zresztą wiele urządzeń, jak tablety i smartfony, nie może być podłączona do sieci przewodowej (LAN). (Tak naprawdę jedynie jeśli potrzebujemy stabilnego i bardzo szybkiego transferu w sieci lokalnej, na przykład pomiędzy komputerem stacjonarnym a serwerem NAS, warto w domu zdecydować się na sieć przewodową – jak Gigabitowy Ethernet, który zapewnia transfer do 125 MB/s przy wykorzystaniu jednego przewodu).

Wszyscy z reguły korzystamy więc z internetu bezprzewodowo. O jednej sprawie musimy jednak pamiętać. **Sieć bezprzewodową trzeba odpowiednio zabezpieczyć.** Jeśli ktoś niepowołany podłączy się do niej, może narobić nam szkód. Pół biedy, jeśli będzie to sąsiad korzystający z naszego internetu, żeby zaoszczędzić na swoim rachunku. Znacznie większe kłopoty może spowodować osoba, która włamie się do naszej sieci w konkretnym celu – na przykład by wykraść dane logowania, choćby do banku lub poczty.

Do zabezpieczenia domowego Wi-Fi możemy podejść na kilka sposobów. Każda metoda podnosi ogólny poziom bezpieczeństwa, dlatego warto krok po kroku uszczelniać swoją sieć. Pamiętajmy, że osoby, które łamią zabezpieczenia, potrafią wykorzystać wiele szczegółów dla większości z nas łatwych do przeoczenia.

Najlepszym kompromisem pomiędzy bezpieczeństwem a łatwością konfiguracji dla użytkowników domowych jest korzystanie z uwierzytelniania typu **WPA2 Personal z szyfrowaniem AES**. Istnieją bardziej bezpieczne rozwiązania, na przykład **WPA2 Enterprise z serwerem RADIUS**, ale dla większości użytkowników konfiguracja takich zabezpieczeń jest zbyt trudna.

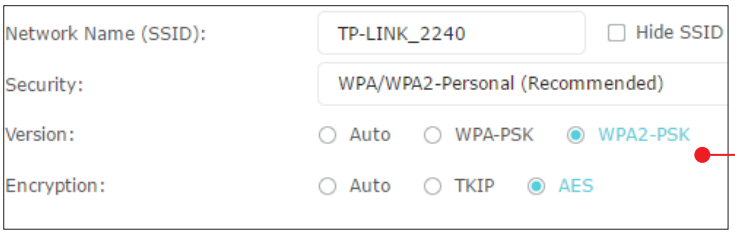
Na kolejnych stronach znajdziemy porady, jak zadbać o bezpieczeństwo naszego Wi-Fi. **kd**

WYBIERAMY PROTOKÓŁ ZABEZPIECZENIA SIECI I SZYFROWANIE

W zależności od modelu rutera możemy spotkać się z różnymi domyślnymi ustawieniami. Nie zawsze są one optymalne pod względem bezpieczeństwa użytkowników. Użytkownicy domowi powinni wybierać protokół **WPA2 Personal** z szyfrowaniem **AES**.

Protokół **WPA** domyślnie korzysta z szyfrowania **TKIP**, podatnego na ataki kryptograficzne, których dość dobrze zoptymalizowane wersje są dostępne w sieci. Jeśli chodzi o zabezpieczenie **WPA-PSK**, to jest ono podatne na specjalnie generowane ataki słownikowe i również nie jest zalecane.

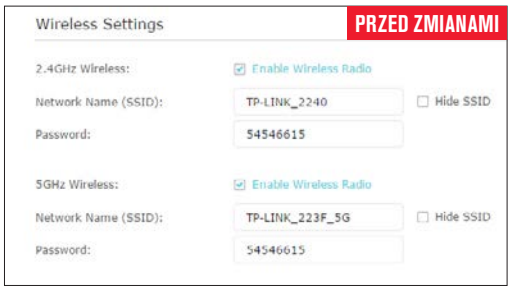
Aby zmienić ustawienia zabezpieczeń sieci, logujemy się do panelu zarządzania rutera i szukamy zakładki **Wireless** lub **Advanced**, **Wireless**, **Wireless Settings**. Potem musimy po prawej stronie wybrać odpowiednie ustawienia i zatwierdzić zmiany. W większości przypadków oznacza to konieczność ponownego zalogowania się na każdym urządzeniu łączącym się z ruterem drogą bezprzewodową.



SIEĆ WI-FI

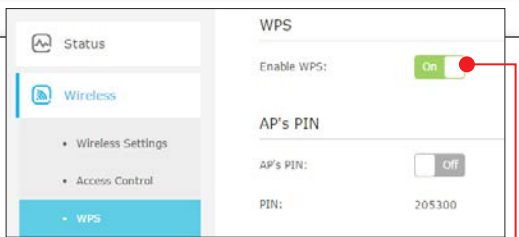
DOMYŚLNE HASŁA DOSTĘPU DO SIECI

Bardzo ważne jest, aby zmienić standardową nazwę sieci bezprzewodowej oraz hasło dostępu. Jeśli nasz ruter udostępnia sieci w dwóch częstotliwościach, dokonujemy zmian dla każdej z nich. Na szczęście w nowych modelach od razu przy pierwszym podłączeniu jesteśmy proszeni o podanie nowego hasła dostępu do urządzenia, jak również o podanie nowego hasła dostępu do sieci bezprzewodowej. Zmiana hasła jest prosta, wystarczy zalogować się do panelu administracyjnego naszego urządzenia, następnie odnaleźć sekcję **Wireless**, a potem podać nowe hasło i zapisać zmiany.



AKTYWNA FUNKCJA WPS

Wiele ruterów domyślnie ma aktywną funkcję **WPS** (**W**i-**F**i **P**rotected **S**etup), co jest potencjalnie niebezpieczne. Funkcja ta pozwala na szybkie, łatwe podłączanie urządzeń do sieci dzięki prostemu kodowi PIN. Sprawia, że możemy podłączać nowe urządzenia bez wpisywania skomplikowanego hasła. Jednak WPS ma luki w zabezpieczeniach i ze względów bezpieczeństwa nie poleca się korzystania z tej opcji. Po pierwsze, luki pozwalają atakującemu na dość proste złamanie zabezpieczenia. Po drugie, zabezpieczenia przed atakami siłowymi na WPS nie dają 100-procentowej ochrony. Dlatego jeśli nie korzystamy z tej opcji, warto ją całkowicie wyłączyć. Po zalogowaniu się do panelu administratora szukamy zakładki Wireless i WPS. Wystarczy wyłączyć opcję **Enable WPS**.



TRUDNE POJĘCIA

Adres MAC
Indywidualny sprzętowy adres karty sieciowej nadawany przez producenta. Można go zmienić.

DHCP
Protokół dynamicznego konfigurowania hostów – protokół komunikacyjny umożliwiający hostom uzyskanie od serwera danych konfiguracyjnych, na przykład adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci.

Serwer Radius
Usługa zdalnego uwierzytelniania użytkowników próbujących połączyć się z siecią, wykorzystywana dla sieci telefonicznych, połączeń tunelowych i sieci bezprzewodowych.

SSID
Service **S**et **I**dentifier – identyfikator sieci składający się z maksymalnie 32 znaków. Pełni rolę loginu do sieci i jednocześnie jej nazwy, którą widzi użytkownik.

Szyfrowanie AES
Advanced **E**ncryption **S**tandard – jest to szyfr blokowy symetryczny, każdy blok składa się ze 128 bitów. Długość klucza może wynosić 128, 192 i 256 bitów. Jest to szyfr wykorzystywany na całym świecie nawet przez agencje amerykańskie do szyfrowania tajnych dokumentów.

Uwierzytelnianie
Proces, który polega na potwierdzeniu tożsamości podmiotu, który bierze udział w procesie komunikacji (na przykład czy komputer A jest w rzeczywistości komputerem A).

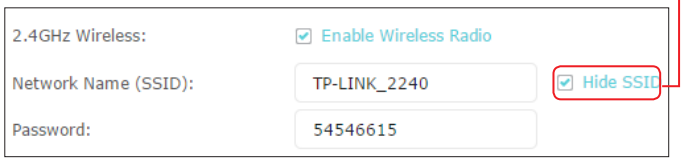
WPA2
Wi-**F**i **P**rotected **A**ccess **2** – protokół zabezpieczenia sieci bezprzewodowych, stosujący szyfrowanie AES, który wykorzystuje dynamiczne, 128-bitowe klucze kryptograficzne, ma poprawione wszystkie luki znalezione w protokole WEP oraz WPA. WPA nie jest bezpieczny od około 2010 roku i zaleca się obecnie stosowanie tylko protokołu WPA2-AES. >

MITY DOTYCZĄCE ZABEZPIECZEŃ SIECI BEZPRZEWODOWYCH

W wielu poradnikach w internecie możemy znaleźć informacje dotyczące zwiększenia zabezpieczeń sieci. Jednak czy wszystkie są prawdziwe? Poznajmy kilka najbardziej popularnych mitów dotyczących zabezpieczeń sieci Wi-Fi

UKRYCIE SSID SIECI

Mit: Praktycznie każdy ruter pozwala na ukrycie identyfikatora sieciowego. Dzięki temu teoretycznie osoba, która nie zna nazwy naszej sieci, nie będzie w stanie się z nią połączyć, nawet jeśli znałaby hasło. Jak jest w rzeczywistości? Jest to **FAŁSZ**.



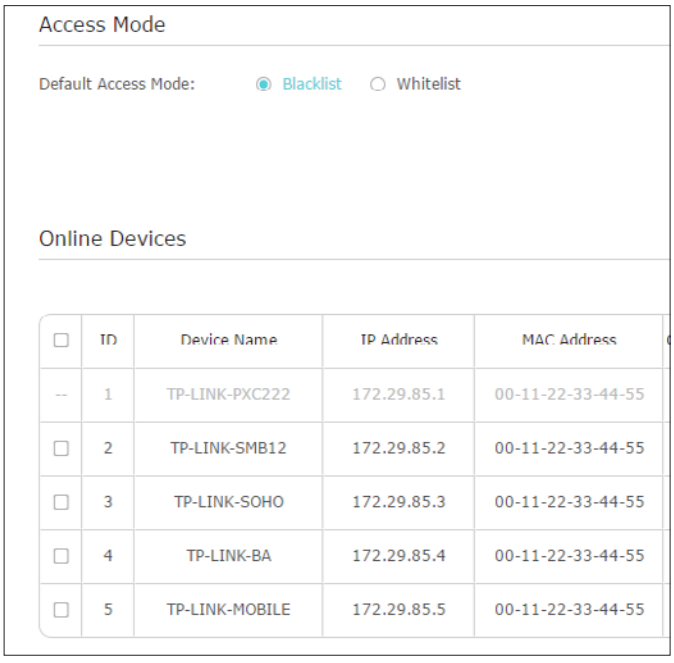
Odkrycie SSID ukrytej sieci nie jest trudne. Wystarczy chwila, jeśli z sieci korzysta aktywnie kilku użytkowników. W dodatku jeśli ukryjemy naszą sieć, stajemy się bardziej podatni na atak. Osoba, która chce poznać hasło sieci, musi tylko utworzyć fałszywy punkt dostępu i sprawić, że rozłączymy się z naszą siecią (co nie jest skomplikowane). Wtedy nasza karta sieciowa w pierwszej kolejności połączy się z widoczną siecią – fałszywą. Zostaniemy poproszeni o podanie hasła i prawdopodobnie odruchowo je podamy, myśląc, że to wymagane, a tym samym zdradzimy swoje zabezpieczenie atakującemu.

WYŁĄCZENIE SERWERA DHCP

Mit: DHCP pozwala ruterowi na dynamiczne przydzielanie adresów IP dla łączących się z siecią urządzeń. Jeśli wyłączymy taki serwer, będziemy mogli przydzielać statyczne adresy IP, indywidualne dla każdego urządzenia. Dzięki temu atakujący po włamaniu się do sieci nie dostanie przydzielonego adresu i nie będzie miał dostępu do naszej domowej sieci. Jest to – w pewnym sensie – **FAŁSZ**.
Z jednej strony w przypadku aktywnego serwera DHCP jesteśmy bardziej podatni na ataki typu **MitM** (**M**an **i**n **t**he **M**iddle – atak polegający na podsłuchu i modyfikacji wiadomości przesyłanych między dwiema stronami bez ich wiedzy) i po włamaniu atakujący od razu ma przydzielony adres. Jednak w przypadku statycznego adresu IP proces połączenia się z siecią może wydawać się trudniejszy, jednak tylko z pozoru. Atakujący może czekać i śledzić pakiety przychodzące i w ten sposób wykryć adresy IP, które pozwalają na uzyskanie dostępu do sieci. Tak więc wyłączenie DHCP znacznie utrudnia zwykłemu użytkownikowi korzystanie z sieci, a nie powstrzyma atakującego, który złamał hasło dostępu do Wi-Fi.

KORZYSTANIE Z FILTROWANIA MAC

Mit: Ponieważ każde urządzenie sieciowe, w tym karty sieciowe, mają unikalne adresy MAC, jeśli wykorzystujemy opcję filtrowania adresów MAC w naszym ruterze i zezwalamy na dostęp tylko wybranym klientom, będziemy bezpieczni, bo nawet jeśli ktoś złamie zabezpieczenia naszej sieci, nie uzyska do niej dostępu. Jest to **FAŁSZ**.
W teorii informacja podana powyżej jest jak najbardziej prawdziwa, jednak jeśli atakujący ma odpowiednią kartę sieciową, bez problemu może przypisać jej dowolny adres MAC. Korzystając z odpowiedniego skanera, bardzo szybko odnajdzie adresy urządzeń, które łączą się z ruterem, zmieni swój adres na jeden z nich, a następnie bez problemu uzyska dostęp do naszej sieci. Nie jest to skomplikowana procedura.
Zatem to rozwiązanie, które jest bardzo uciążliwe dla korzystającego na co dzień z rutera, nie jest dużym utrudnieniem dla doświadczonego atakującego. Filtrowanie MAC może spełnić swoje zadanie w przypadku, gdy naszą sieć atakuje amator.



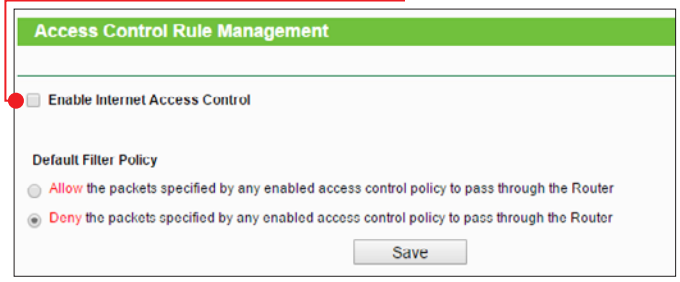
JAKIE DODATKOWE KROKI MOŻEMY PODJĄĆ, BY POPRAWIĆ BEZPIECZEŃSTWO SIECI

WYŁĄCZAMY ZDALNY DOSTĘP DO RUTERA

Obecnie ta funkcja jest domyślnie wyłączona w większości nowych urządzeń – ale warto się co do tego upewnić.

Funkcja ta pozwala na uzyskanie dostępu do rutera z zewnątrz, z internetu. Oznacza to, że jeśli ktoś zna nasz publiczny adres IP, a nasze urządzenie ma lukę w zabezpieczeniach, atakujący może uzyskać w łatwy sposób dostęp do naszego rutera oraz do całego ruchu generowanego przez naszą sieć.

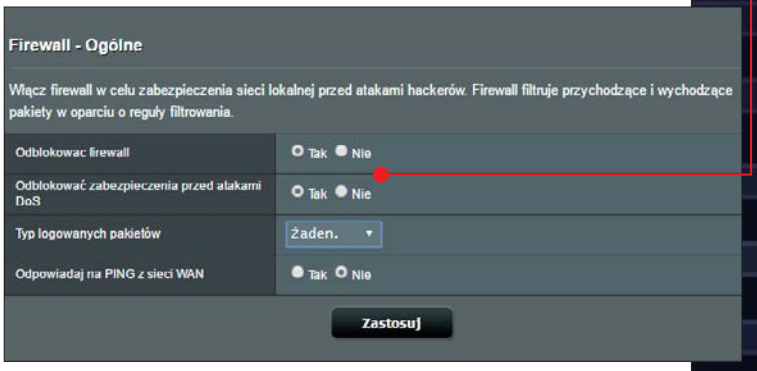
Jeśli chcemy sprawdzić stan tej opcji, logujemy się do panelu zarządzania ruterem oraz szukamy zakładki **Access Control**. W niej znajdziemy opcję dostępu do rutera z internetu. Powinna być wyłączona.



USTAWIENIA FIREWALLA

Domyślnie zdecydowana większość ruterów ma wyłączone specjalistyczne zabezpieczenia przed atakami DoS, ponieważ niepotrzebnie zużywają zasoby urządzenia i bardzo rzadko klient indywidualny jest narażony na tego typu atak.

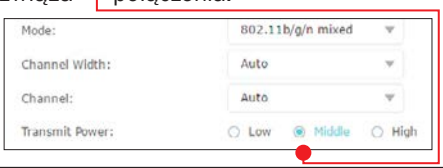
Jednak jeśli chcemy czuć się bardziej bezpiecznie, możemy aktywować wszystkie zabezpieczenia – tak naprawdę mało kto zużywa wszystkie zasoby swojego rutera, a dodatkowe aktywne zabezpieczenie zawsze może się przydać. Odpowiednie ustawienia najczęściej znajdziemy w zakładce **Security**, **Firewall** – wystarczy tylko je aktywować.



ZMNIEJSZENIE MOCY NADAWANIA

Jest to dość niecodzienne rozwiązanie, dzięki któremu zmniejszamy moc sygnału nadawanego przez nasz ruter. Co to daje? Uniemożliwia na przykład osobie z laptopem, choćby w samochodzie niedaleko naszego domu, podpięcie się do naszej sieci – po prostu nie będzie odpowiedniego zasięgu. Nie wszystkie urządzenia pozwalają na takie rozwiązanie, musimy też zdawać sobie sprawę, że ograniczamy przepustowość naszej sieci, jeśli nasze urządzenia nie będą pracowały z maksymalnym zasięgiem.

Takie ustawienia znajdziemy najczęściej w zakładce **Advanced**, **Wireless**, **Wireless Settings**. Musimy odszukać pole **Transmit Power** lub **Rx Power**. Należy odpowiednio zmniejszyć moc, tak aby w naszym domu zasięg był dobry, a poza jego murami obce osoby nie mogły uzyskać połączenia.



KORZYSTANIE Z PUBLICZNYCH SIECI BEZPRZEWODOWYCH

Jeśli zależy nam na bezpieczeństwie, musimy pamiętać o tym, że kiedy korzystamy z publicznych punktów dostępu, należy odpowiednio zabezpieczyć się przed różnego typu atakami. Największe ryzyko niesie za sobą możliwość „podsłuchiwania" pakietów danych, które wychodzą i przychodzą do naszego urządzenia. Jeżeli nie musimy, nie logujemy się do ważnych kont – bankowych, pocztowych itp. Więcej o zachowaniu bezpieczeństwa w otwartych sieciach przeczytamy w poradniku na stronie 62, znajdziemy tam też informacje o ryzyku związanym z utratą anonimowości i kradzieżą danych w sieciach publicznych.

KONFIGURACJA RUTERA

O podstawowej konfiguracji rutera przeczytamy w tym wydaniu w poradniku na stronie 64.

Fot. Frank Peters, Mipan/123rf.com

TRIKI
DO INTERNETU
JAK SIĘ BRONIĆ PRZED HAKERAMI

ATAKI W SIECI DOMOWEJ

Ataki, na jakie narażona jest sieć domowa, można podzielić na dwie główne kategorie – wyróżniamy ataki **pasywne** i **aktywne**. Te pierwsze polegają na zbieraniu informacji: śledzeniu, podsłuchiwaniu, analizie ruchu sieciowego. Prowadzą one do właściwego ataku aktywnego, którego celem jest modyfikacja danych użytkownika, przejęcia kontroli nad jego urządzeniem lub zakłócenie jego pracy.

Jak powstrzymać hakera

Oczywiście, zaawansowani hakerzy korzystają z nowych, skomplikowanych sposobów włamań – jest ich jednak niewielu. Znacznie więcej jest zwykłych amatorów, którzy wykorzystują najprostsze sposoby włamań, takie, które można łatwo zablokować, gdy zna się procedury najczęstszych ataków. Jeśli chcemy zabezpieczyć się przed atakiem, powinniśmy zacząć myśleć jak haker. Trzeba zadać sobie pytanie: jakie są możliwości infiltracji sieci, przejęcia kontroli nad pakietami sieciowymi lub urządzeniami? Tak naprawdę najważniejsze jest zabezpieczenie sieci bezprzewodowej, ponieważ jeśli intruz uzyska do niej dostęp, zyska możliwość wykonania ataku. Największym zagrożeniem jest właśnie złamanie zabezpieczeń sieci domowej, bo otwiera furtkę do kolejnych ataków i pozwala przejąć nasze dane.

Do włamania się do sieci bezprzewodowej najczęściej wykorzystywane jest narzędzie **aircrack-ng**. Umożliwia ono łamanie zabezpieczeń sieci, a jedyna ochrona przed nim to silne hasło. Znając adres IP i e-mail ofiary, atakujący także może próbować ataku, jednak w takim wypadku wystarczy nie otwierać podejrzanych plików i nie instalować niebezpiecznych programów, by móc czuć się w miarę bezpiecznie. **kd**

ATAKI PASYWNE

W tej kategorii możemy wyróżnić kilka przykładów takich ataków:

→ Social Engineering

Jest to sposób na pozyskanie wrażliwych danych, wykorzystujący ludzką lekkomyślność i brak wiedzy. Atakujący wysyłają fałszywe e-maile, przeglądają wyrzuconą dokumentację, podglądają użytkowników przy logowaniu itp.

→ Skanowanie sieci

Ta metoda pozwala na poznanie szczegółów dotyczących atakowanej sieci, by dowiedzieć się, jakie urządzenia z niej korzystają, które porty są otwarte itp.

→ Sniffing

Ten atak pasywny polega na monitorowaniu i rejestrowaniu całego ruchu sieciowego lub jego części w atakowanej sieci. Odpowiednio wykonany może umożliwić odkrycie haseł, loginów, a nawet prywatnych rozmów użytkowników.

→ Łamanie hasła

Łamanie hasła w sposób niezauważalny dla użytkownika też jest uważane za atak pasywny. Dzięki tej metodzie atakujący, korzystając z metody siłowej (brute-force), może złamać zabezpieczenie, wystarczy odpowiednio dużo czasu i mocy obliczeniowej.

ATAKI AKTYWNE

Tego typu ataków jest znacznie więcej niż pasywnych, poniżej wymieniono tylko te najważniejsze.

→ Spoofing

Ten typ ataku polega na podszywaniu się pod inny autoryzowany w danej sieci komputer. Celem jest oszukanie systemów zabezpieczających, umożliwia to bezproblemowe uzyskanie dostępu na przykład do sieci, w której aktywne jest filtrowanie MAC.

→ Hijacking

To przechwytywanie sesji w protokole TCP. Dzieje się to po tym, jak atakujący zrywa połączenie między serwerem i klientem, aby móc zastąpić klienta i bez konieczności logowania kontynuować komunikację.

→ Koń trojański

Popularnie nazywany trojanem. Jest to program, który może podszywać się pod zaufaną aplikację lub wchodzić w jej skład. Po zainstalowaniu przez użytkownika trojan wykonuje w tle operacje, które zaprogramował atakujący, na przykład zapisuje hasła lub inne dane.

→ Ataki typu DoS

Jest to typ ataków, które mają na celu uniemożliwienie użytkownikom dostępu do usług. Polegają głównie na spamowaniu połączeń i mają za zadanie wyczerpać zasoby serwera lub dowolnego urządzenia sieciowego, czego skutkiem ma być przerwanie pracy danego urządzenia.

Bezpieczeństwo w naszej sieci powinno być dla nas najważniejsze. Dlatego warto znać metody, jakie wykorzystują hakerzy i crackerzy, by włamywać się do sieci. Poznajmy ***najpopularniejsze typy ataków i sposoby na obronę*** *przed nimi*

WARTO WIEDZIEĆ

Atak słownikowy
Próba złamania hasła przy wykorzystaniu obszernej listy możliwych haseł. Słowniki mogą osiągać bardzo duże rozmiary. Z reguły są kompilacją najczęściej wykorzystywanych statystycznie haseł oraz kombinacji wyrazów ze słowników językowych.

Firewall
Zapora ogniowa. Zabezpieczenia takie nie wpuszczają szkodników do sieci. Oprogramowanie to określa, jakie dane są autoryzowane. Zazwyczaj jest ono umieszczone w ruterach lub serwerach dedykowanych.

MitM
Man **i**n **t**he **M**iddle – atak kryptologiczny polegający na podsłuchu i modyfikacji wiadomości przesyłanych między dwiema stronami bez ich wiedzy. Atakujący może spowodować, że dane z naszego komputera będą przechodziły przez jego komputer, a dopiero później trafią do serwera zewnętrznego.

Tablice tęczowe
Specjalnie kompilowane obszerne bazy skrótów możliwych haseł. Zwykłe tablice zajmują nawet kilkaset gigabajtów danych – tablica tęczowa zapisana przy wykorzystaniu łańcuchów pozwala zaoszczędzić przestrzeń dyskową i skrócić czas łamania haseł o kilkaset procent.

PRZYKŁADOWY ATAK HAKERA KROK PO KROKU

1 Włamanie się do sieci Wi-Fi z wykorzystaniem narzędzia **aircrack-ng**.

2 Skanowanie sieci w poszukiwaniu celów ataku i sprawdzanie, które porty są otwarte – narzędzie **Nmap**.

3 Jeśli system jest niezabezpieczony lub ma luki w zabezpieczeniach, możliwe, że bez większego trudu uda się uzyskać dostęp z wykorzystaniem narzędzia **Metasploit**. Jeżeli nie, atakujący szuka innego punktu zaczepienia.

4 Podsłuchiwanie sieci, analizowanie całego ruchu w celu wychwycenia haseł dostępu, adresów e-mail i innych wrażliwych danych – narzędzie **Wireshark**.

5 Atak drogą e-mailową za pomocą **Metasploit** lub innych podobnych narzędzi.

6 Instalacja na urządzeniu ofiary backdoora, czyli utworzonej przez atakującego luki w zabezpieczeniach, która umożliwia dostęp do urządzenia, gdy jest ono dostępne w sieci, w celu utrzymania nad nim kontroli.

SIŁA HASŁA A CZAS POTRZEBNY NA JEGO ZŁAMANIE

Najczęściej wybieraną metodą zabezpieczenia sieci Wi-Fi jest wykorzystanie uwierzytelniania typu **WPA2 Personal** oraz szyfrowania **AES**. Siła naszego hasła zależy jednak znacznie bardziej od jego złożoności i liczby użytych znaków. Oto zestawienie, które zakłada wykorzystanie zwykłej siłowej metody łamania hasła, a nie słownika czy tablic tęczowych (patrz słowniczek powyżej).

Pula znaków, z których można utworzyć hasło	Liczba znaków hasła	Liczba kombinacji	Czas potrzebny na złamanie hasła (komputer ze specjalnym programem, dla szybkości 1 x 10^9/s kluczy)
10 (liczby)	8	1×10^8	~2 minut
26 (małe lub duże litery)	8	2×10^{11}	~2,5 dnia
52 (małe i duże litery)	8	$5{,}3 \times 10^{13}$	~1,5 roku
62 (litery i cyfry)	8	$2{,}2 \times 10^{14}$	~7 lat
96 (wszystkie dostępne znaki)	8	$7{,}2 \times 10^{15}$	~229 lat

Podany czas to czas maksymalny potrzebny na znalezienie hasła, a zastosowanie słowników znacząco przyspiesza możliwość złamania hasła typowego użytkownika. Dlatego należy tworzyć jak najdłuższe hasła, składające się z różnych znaków, cyfr i symboli – wtedy będą praktycznie nie do złamania.
Szybkość łamania hasła podana jest dla typowego konsumenckiego komputera z podzespołami dobrej klasy.

Fot. ra2studio/123rf.com

ŁAMANIE ZABEZPIECZEŃ SIECI WI-FI

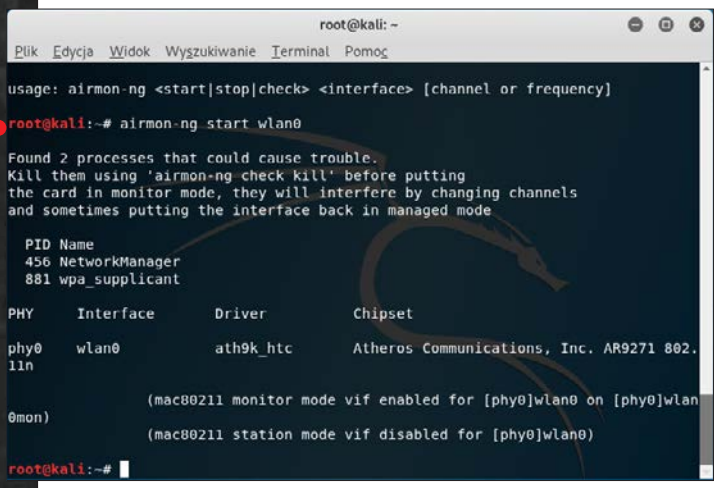
Wiemy już, że bezpieczna sieć to odpowiednie hasło i typ uwierzytelniania. Przeczytajmy teraz, jak samemu sprawdzić siłę naszego hasła, wykorzystując narzędzia dostępne w systemie **Kali Linux** (DVD-KOD: **022**) przeznaczonym specjalnie do testów penetracyjnych, czyli do weryfikowania różnego rodzaju zabezpieczeń w sieci i na komputerach.

Wykorzystamy specjalny pakiet **aircrack-ng** wchodzący w skład systemu Kali Linux. Pakiet ten składa się z kilku narzędzi mających jasny i określony cel – analiza sieci bezprzewodowych i łamanie ich zabezpieczeń. W internecie znajduje się lista adapterów i kart sieciowych, które są zatwierdzone przez twórców tego programu. Nie będziemy mogli z niego korzystać na typowej karcie sieciowej w laptopie, ponieważ takie karty nie zapewniają obsługi trybu monitora, który jest niezbędny do wykonania ataku – musimy mieć kompatybilny moduł sieciowy.

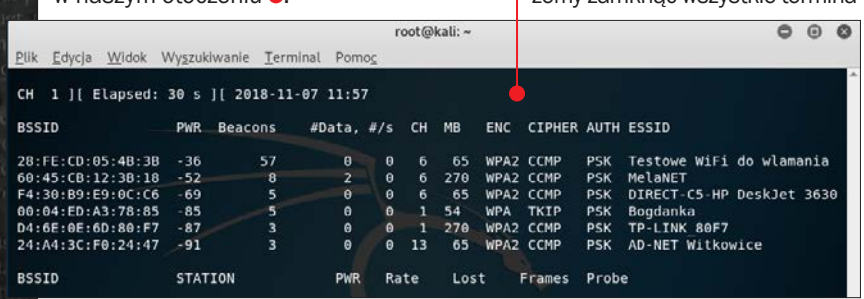
```
root@kali:~# aircrack-ng Plik1-01.cap -w /usr/share/wordlists/nmap.lst
```

```
root@kali:~# airodump-ng --bssid 28:FE:CD:05:4B:3B -c 6 --write Plik1 wlan0mon
```

1 Po uruchomieniu systemu Kali Linux i podłączeniu odpowiedniego adaptera sieciowego uruchamiamy terminal, wpisujemy komendę: **airmon-ng start wlan0** i zatwierdzamy ją klawiszem enter. Uruchomi to tryb monitora **wlan0mon** na karcie Wi-Fi i pozwoli na skanowanie w poszukiwaniu sieci.



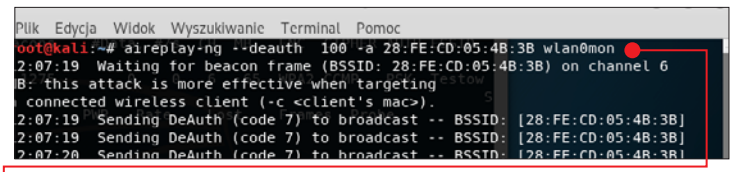
2 Następnie wpisujemy **airodump-ng wlan0mon** – rozpocznie to skanowanie sieci w naszym otoczeniu.

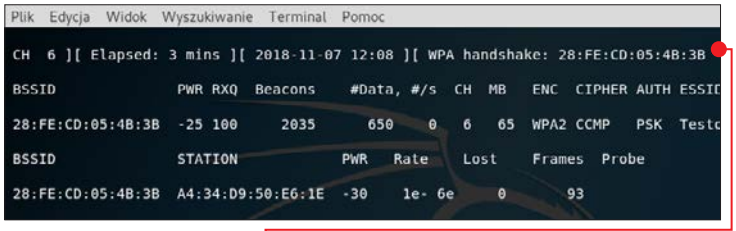


3 Dzięki temu będziemy mogli dowiedzieć się między innymi, jak zabezpieczone są poszczególne sieci. My oczywiście „włamujemy się" do naszej sieci, do której znamy hasło – czyli **Testowe WiFI do włamania**.

4 Musimy wpisać komendę **airodump-ng --bssid XX:XX:XX:XX:XX -c X --write Plik1 wlan0mon**. Zamiast **X** podajemy dane naszej sieci, które są widoczne na ekranie w punkcie **2**. BSSID znajdziemy w pierwszej kolumnie, a **c** to oznaczenie kanału, czyli kolumna **CH**.

5 Teraz musimy przechwycić zakodowane hasło dostępu do sieci. Uda się to wtedy, gdy jakiś użytkownik połączy się z tą siecią lub my wymusimy rozłączenie użytkownika, który za chwilę automatycznie się z nią połączy, a my będziemy mogli wtedy przechwycić zakodowane hasło.





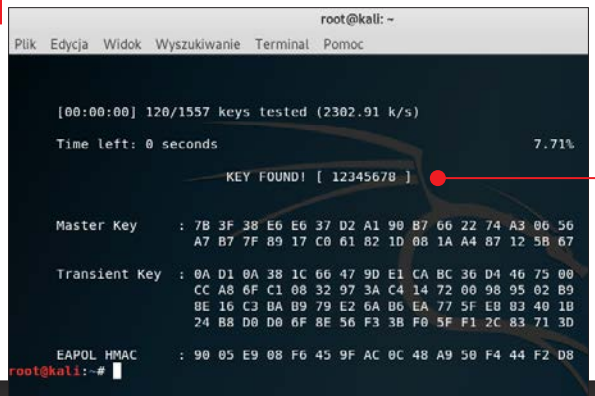
6 W nowym oknie terminalu wpisujemy komendę **aireplay-ng --deauth 100 -a XX:XX:XX:XX:XX:XX wlan0mon**, ponownie w miejsce **X** podajemy dane rutera.

7 Teraz w głównym oknie z punktu **4** w prawym górnym rogu powinien pojawić się napis **WPA Handshake** oraz adres MAC punktu dostępowego. Możemy zamknąć wszystkie terminale, ponieważ zaszyfrowane hasło jest już zapisane w pliku **Plik1** na naszym komputerze.

8 Następnie musimy w nowym terminalu wpisać komendę **aircrack-ng Plik1-01.cap -w [lokalizacja słownika]** i zatwierdzić. Rozpocznie się wtedy łamanie hasła metodą słownikową. Łamanie hasła tą metodą może być bardzo czasochłonne i nieefektywne. Jeśli hasła nie ma w słowniku, nie zostanie znalezione.

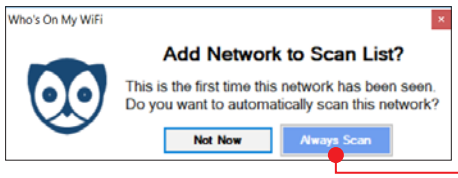
9 W przypadku tego specjalnie ustalonego hasła **12345678** czas łamania był bardzo krótki, ponieważ jest to proste hasło i było zawarte w słowniku. Średniej klasy komputer sprawdza około 2000 haseł na sekundę.

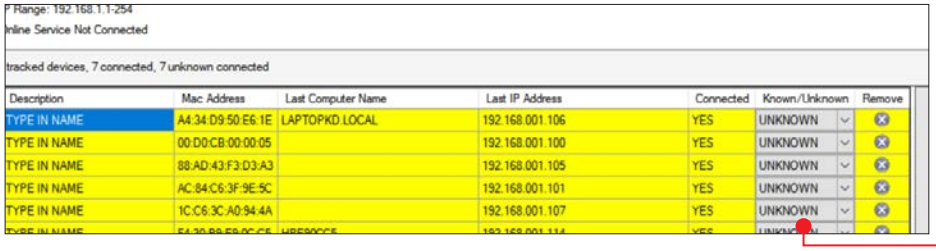
Cały ten proces jest dość trudny i skomplikowany, możemy jednak wyciągnąć z tego naukę – im dłuższe i bardziej złożone hasło, tym trudniejsze jest do złamania. Zaleca się stosowanie hasła przynajmniej 16-znakowego, składającego się z małych i dużych liter, cyfr oraz znaków specjalnych. Takie hasło jest prawie nie do złamania, dzięki czemu będziemy bezpieczni. Nie ma sensu stosować filtrowania adresów MAC, gdyż atakujący może w krótkim czasie podszyć się pod nasz adres MAC i dostać do sieci, korzystając z opisanej metody. Solidne hasło to najważniejszy punkt obrony.



SPRAWDZAMY, CZY KTOŚ OBCY NIE KORZYSTA Z NASZEGO WI-FI

W tym celu wykorzystamy program **Who Is On My WiFi**, który można pobrać z KŚ+ (www.ksplus.pl). Dzięki niemu będziemy mogli w czasie rzeczywistym skanować naszą sieć i na bieżąco będziemy widzieli informacje o tym, jakie urządzenia z niej korzystają. Po dodaniu zaufanych urządzeń pozwoli to na łatwe rozpoznanie intruza.





1 Po zainstalowaniu programu klikamy na **Scan Now** w prawym górnym rogu.

2 Następnie klikamy na opcję **Always Scan**.

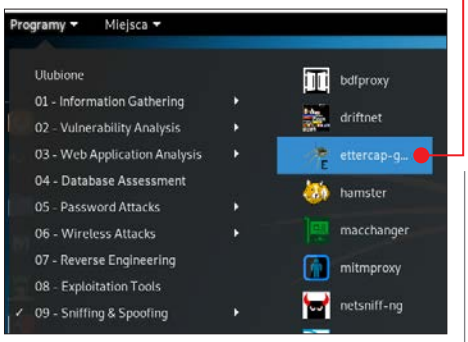
3 Po chwili skanowanie zostanie zakończone, a wszystkie znalezione urządzenia zobaczymy w głównym oknie interfejsu programu. Wystarczy zweryfikować adresy IP naszych urządzeń i zmienić ich status z **Unknown** na **Known**.

4 Program będzie działał w tle i wykonywał skanowania co 5 minut. Jeśli znajdzie jakieś nowe urządzenie, które podłączy się do naszej sieci, czyli potencjalnego intruza, dostaniemy powiadomienie. Będziemy wtedy musieli jak najszybciej zmienić hasło dostępu do sieci.

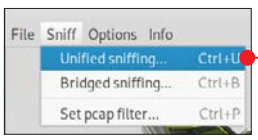
JAK DZIAŁA SNIFFING

Wykorzystując narzędzie **Ettercap** z systemu Kali Linux, możemy również sprawdzić, jak wygląda typowy atak typu sniffing, który polega na podsłuchiwaniu pakietów i wychwytywaniu z nich kluczowych danych.

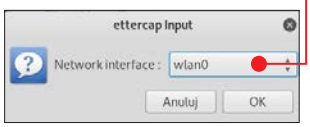
1 Uruchamiamy program Ettercap – klikamy na **Programy**, **09 Sniffing & Spoofing**, **Ettercap gui**.



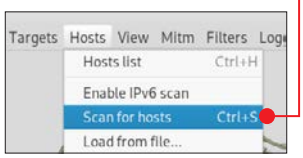
2 Klikamy na **Sniff**, **Unified Sniffing**.



3 Wybieramy interfejs do tego zadania, w naszym przypadku **wlan0**.

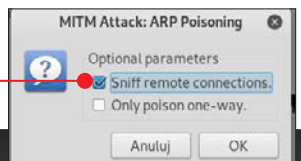


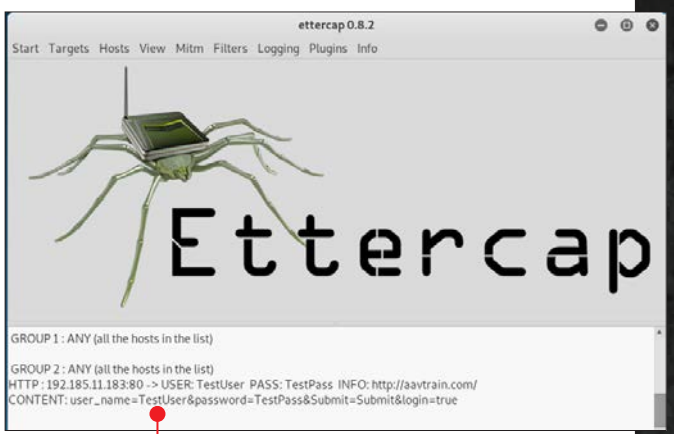
4 Teraz klikamy na **Hosts**, **Scan for Hosts**.



5 Następnie klikamy na **Mitm**, **ARP Poisoning**.

6 Zaznaczamy opcję **Sniff remote connections** i klikamy na **OK**.





7 Teraz na dole ekranu będziemy mogli obserwować, jakie hasła i adresy zostają przechwycone. Dzięki temu dowiemy się, które witryny i programy nie oferują wystarczającej ochrony.

Przedstawiony przykład pokazuje, jak łatwo wychwycić dane w przypadku korzystania z protokołu HTTP. Jeśli będziemy się łączyć z witrynami, wykorzystując protokół HTTPS i na pasku przeglądarki będzie ikona kłódki, możemy mieć pewność, że dane są szyfrowane i po przechwyceniu haker nie będzie miał z nich pożytku.

TRIKI
DO INTERNETU
NAJLEPSZE PROGRAMY DO POPRAWIANIA WI-FI

ZBADAJ SW

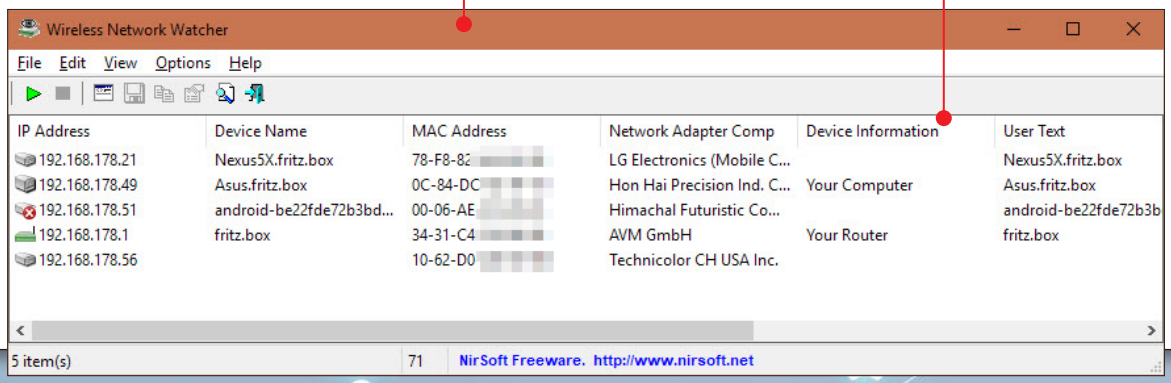
Sprawne działanie sieci bezprzewodowej zależy od wielu czynników: siły sygnału, zasięgu, kanału, na jakim sieć pracuje, liczby sieci Wi-Fi funkcjonujących w najbliższym otoczeniu itp. Warto posłużyć się ***narzędziami, które dostarczą informacji na temat naszej domowej sieci Wi-Fi****, a także wszystkich sieci działających w sąsiedztwie*

WIRELESS NETWORK WATCHER – CO JEST PODŁĄCZONE DO NASZEGO WI-FI?

Wireless Network Watcher (DVD-KOD: **068**) – niewielki, bezpłatny program dla Windows (w dowolnej wersji), bardzo proste w obsłudze narzędzie, które szybko ujawni nam, jakie urządzenia są podłączone do naszej domowej sieci Wi-Fi. Wireless Network Watcher nie skanuje innych sieci, bada jedynie tę, do której podłączony jest komputer, na którym uruchomimy aplikację.

1 Po instalacji i uruchomieniu programu zobaczymy niewielkie okno z kilkoma wpisami. Każdy wpis odpowiada za jedno urządzenie funkcjonujące w naszej domowej sieci Wi-Fi.

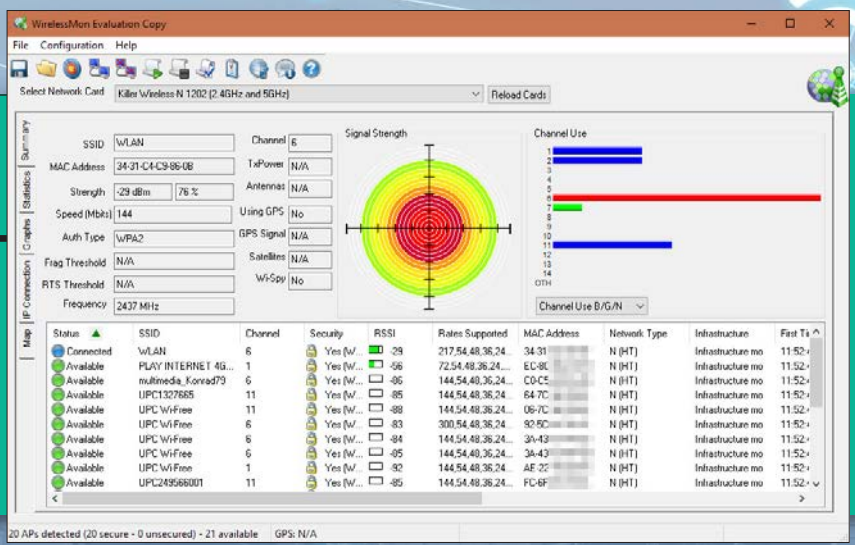
2 W kolejnych kolumnach otrzymujemy informacje o: lokalnym adresie IP (przypisywanym przez ruter) danemu urządzeniu, nazwie urządzenia (pod jaką jest widoczne w danej sieci), adresach MAC podłączonych sprzętów i producencie interfejsu sieciowego. Dodatkowo w kolumnie **Device Information** program podpowiada, które z urządzeń jest komputerem, na którym uruchomiono aplikację, a które to ruter domowej sieci Wi-Fi.



Ta prosta aplikacja pozwala łatwo sprawdzić, czy z naszej sieci nie korzysta ktoś nieuprawniony. Jeżeli jakiekolwiek urządzenie budzi nasze podejrzenia, warto zadbać przynajmniej o zmianę hasła dostępowego do rutera.

MONITOROWANIE WI-FI NA KOMPUTERZE

Do sprawdzenia, jakie sieci Wi-Fi działają w okolicy, najwygodniej posłużyć się aplikacją mobilną, ale można też skorzystać z programu instalowanego na komputerze z Windows, takiego jak **Passmark WirelessMon 4** (DVD-KOD: **043**). Narzędzie to pozwala nie tylko monitorować działające w najbliższym otoczeniu sieci Wi-Fi, ale też dostarcza bardzo wiele statystyk dotyczących parametrów sieci bezprzewodowych. Program dostępny jest w 30-dniowej wersji próbnej.



OJE WI-FI

NA NASZYM DVD

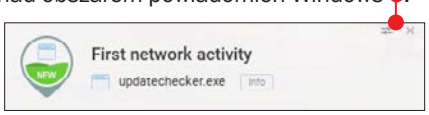
GLASSWIRE – JAKIE APLIKACJE ŁĄCZĄ SIĘ Z SIECIĄ?

Aplikacja **GlassWire** (DVD-KOD: **018**) to narzędzie pozwalające monitorować, jakie aplikacje i usługi zainstalowane w systemie korzystają z naszej sieci. Dzięki tej aplikacji dowiemy się, jakie programy próbują komunikować się z internetem, a także ile danych wysyłają i z jakimi serwerami się łączą.

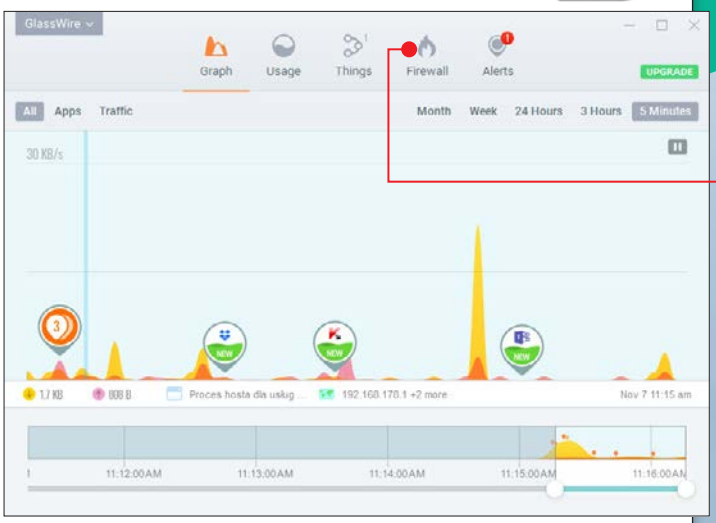
1 Po zainstalowaniu programu i jego uruchomieniu automatycznie rozpocznie on monitorowanie aktywności sieciowej. W oknie aplikacji zobaczymy wykres z charakterystycznymi symbolami określającymi konkretne aplikacje próbujące łączyć się z siecią po raz pierwszy. Sporo tych elementów pokazuje się bezpośrednio po instalacji GlassWire, kiedy to większość usług będzie się łączyć

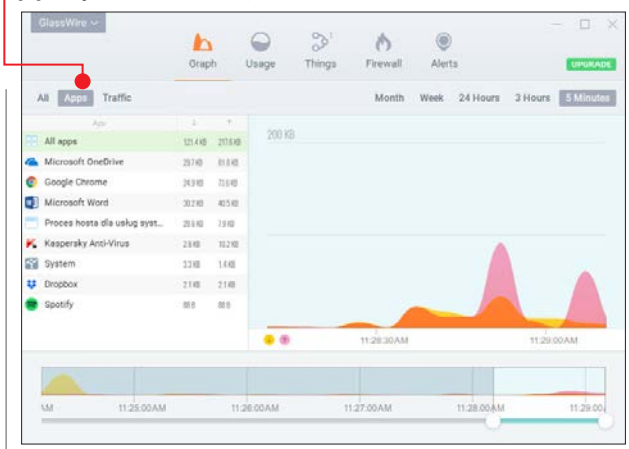
dla programu po raz pierwszy. Kliknięcie na taki symbol aplikacji wyświetli okno z informacjami na temat typu aktywności, nazwy aplikacji oraz docelowego adresu serwera, z którym nastąpi połączenie.

2 Program GlassWire działa w tle, przypominając zaporę ogniową. W sytuacji gdy pojawi się jakakolwiek nowa, nieznana wcześniej aktywność, zobaczymy niewielki komunikat nad obszarem powiadomień Windows.



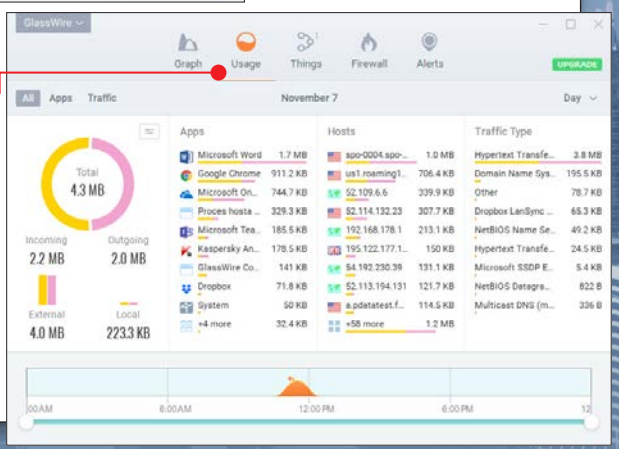
3 W każdej chwili możemy również sprawdzić bieżącą aktywność sieciową działających w systemie aplikacji. Wystarczy w module **Graph** (domyślnie otwartym) kliknąć na przycisk **Apps**. Zobaczymy wtedy tabelkę z nazwami aplikacji oraz wygenerowanym przez nie ruchem przychodzącym (strzałka w dół) i wychodzącym (strzałka w górę). Wybierając dowolną aplikację z listy, zobaczymy wykres pokazujący jej aktywność sieciową.





4 Interesujące dane uzyskamy po kliknięciu w oknie GlassWire na ikonę **Usage**. Zobaczymy wtedy informacje na temat ilości danych przesłanych przez sieć przez poszczególne aplikacje i serwery. Oprócz tego (trzecia kolumna z listą **Traffic Type**) program pokazuje, jakiego typu ruch jest generowany.

5 W kontekście bezpieczeństwa szczególnie interesującą funkcją jest **Firewall**. Po kliknięciu na w oknie programu nie tylko wyświetlane są wtedy nazwy aplikacji i usług korzystających z dostępu do internetu, ale również pojawia się możliwość zablokowania dowolnej aktywności. Obok każdego wpisu widoczny jest symbol płomienia. Gdy na niego klikniemy, zostanie on przekreślony, co oznacza, że jakikolwiek ruch sieciowy inicjowany przez tę aplikację bądź połączony z nią serwer jest blokowany.



MOBILNE MONITOROWANIE SIECI WI-FI

Bardzo dobrym narzędziem do monitorowania siły sygnału i zasięgu sieci Wi-Fi jest smartfon z zainstalowanymi odpowiednimi aplikacjami mobilnymi. Warto wypróbować szczególnie dwie użyteczne aplikacje: **WiFi Analyzer** (VREM Software Development) oraz **Wifi Analyser** (Keuwlsoft).

Android*

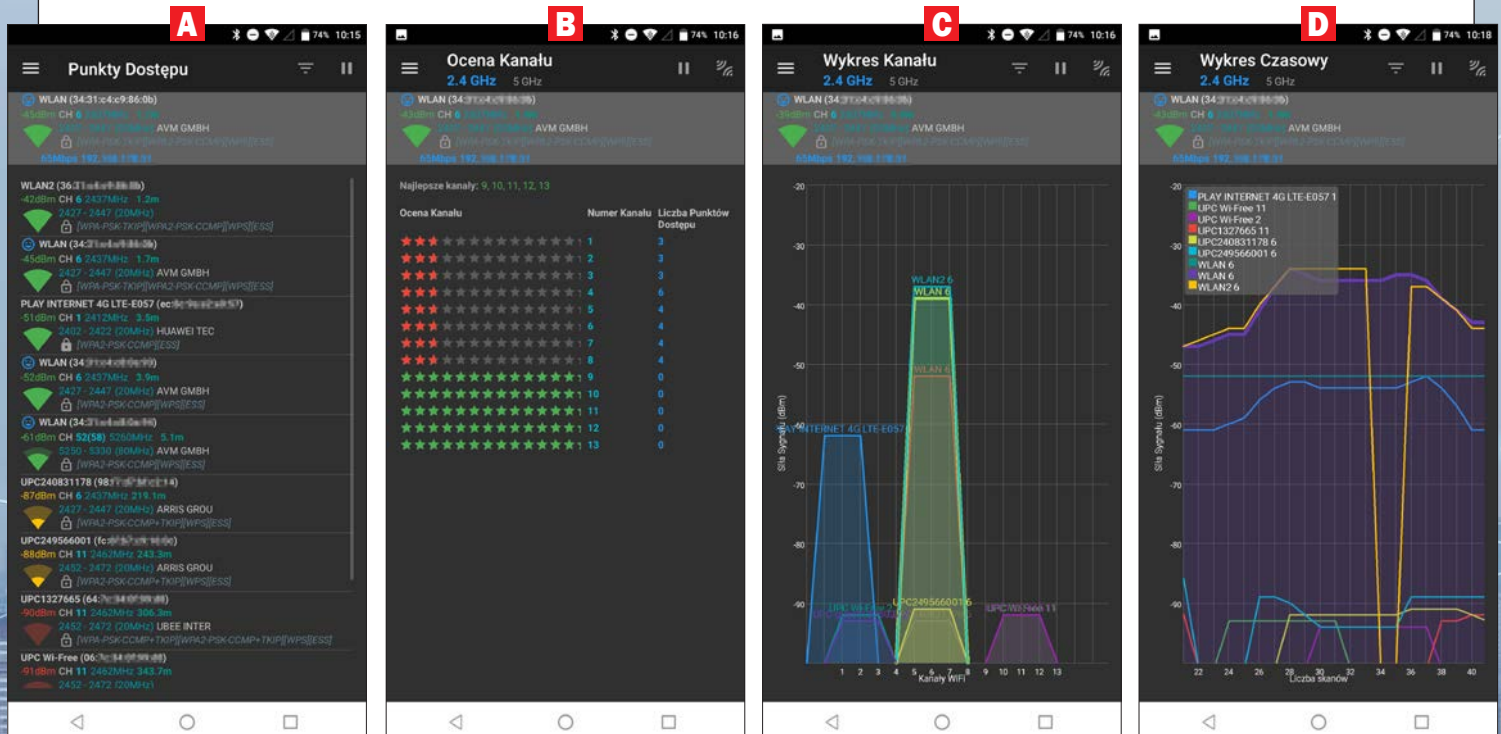
WIFI ANALYZER – SPRAWDZAMY SIECI

WiFi Analyzer dostępny jest w oficjalnym sklepie Google Play, jest bezpłatny i na licencji Open Source. Za jego pomocą możemy sprawdzić parametry wszystkich sieci Wi-Fi działających w bezpośrednim otoczeniu.

1 Po zainstalowaniu i uruchomieniu aplikacji w smartfonie domyślnie na ekranie zobaczymy wyświetlone parametry wszystkich wykrytych przez smartfon sieci bezprzewodowych **A**. Dla każdej sieci aplikacja podaje takie parametry, jak siła sygnału (ujemna wartość w decybelach, im bliższa zeru, tym sygnał jest silniejszy), kanał Wi-Fi, na którym dana sieć pracuje, czy numer MAC interfejsu sieciowego w danym ruterze/punkcie dostępowym. Oprócz tego program wyświetla również informacje o poziomie zabezpieczeń (zalecany to WPA2-PSK). Listę wyświetlonych sieci możemy filtrować według kilku parametrów, takich jak: pasmo (2,4 GHz, 5 GHz), nazwa (SSID), określony poziom siły sygnału czy poziom zabezpieczeń.

2 Przydatną funkcją jest **Ocena Kanału** **B** (taką pozycję należy wybrać w menu aplikacji wywoływanym dotknięciem ikony menu w lewym, górnym rogu interfejsu aplikacji). Program wyświetli wtedy listę wszystkich dozwolonych kanałów Wi-Fi dla konkretnego pasma (domyślnie 2,4 GHz; pasmo zmieniamy, wskazując wartość w górnej części ekranu). Oprócz tego każdy kanał jest oceniony gwiazdkami, a po prawej stronie widoczna jest liczba punktów dostępowych pracujących na danym kanale. Im więcej urządzeń korzysta z tego samego kanału, tym gorzej (wzajemnie się zakłócają). Dzięki temu bardzo łatwo zobaczyć, które kanały są najmniej zatłoczone – na nich warto ustawić własny ruter w razie kłopotów z działaniem sieci.

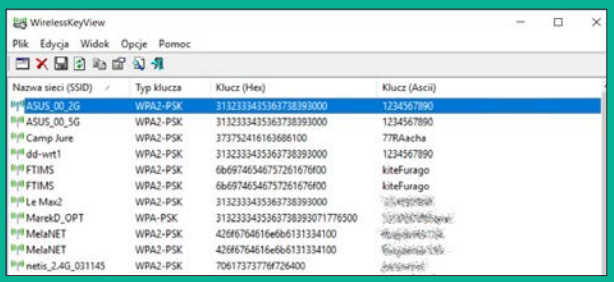
3 Wybierając z menu pozycję **Wykres Kanału** **C**, zobaczymy wykres pokazujący siłę sygnałów sieci Wi-Fi w ramach kanałów, na jakich te sieci pracują. Natomiast gdy wybierzemy z menu aplikacji pozycję **Wykres Czasowy** **D**, na ekranie pojawi się generowany w czasie rzeczywistym wykres obrazujący siłę sygnału sieci. Ponieważ ten wykres jest tworzony na bieżąco, nadaje się do sprawdzenia, w którym miejscu naszego domu sygnał naszej sieci jest najsłabszy czy najsilniej zakłócany przez sąsiadujące sieci.



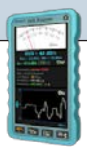
WIRELESSKEYVIEW – GDY ZAPOMNIAŁEŚ HASŁA DO WI-FI

WirelessKeyView (DVD-KOD: 069) to prosty w obsłudze program, który wyświetla informacje o nazwach (SSID) i hasłach do wszystkich sieci Wi-Fi, z jakimi komputer, na którym uruchamiamy tę aplikację, kiedykolwiek się połączył. Dzięki temu w sytuacji, gdy zapomnimy hasła do sieci, a będziemy chcieli podłączyć do niej nowe urządzenie, nie będziemy musieli resetować ustawień rutera. Wystarczy uruchomić WirelessKeyView na dowolnym komputerze, który ma już połączenie z daną siecią, i z okna programu odczytać hasło dostępowe.

W przypadku sieci domowej możemy też sprawdzić hasło, logując się do panelu administracyjnego rutera i sprawdzając za jego pośrednictwem ustawienia naszego Wi-Fi.



WIFI ANALYSER – SZYBKIE MIERZENIE SIŁY SYGNAŁU



Android*

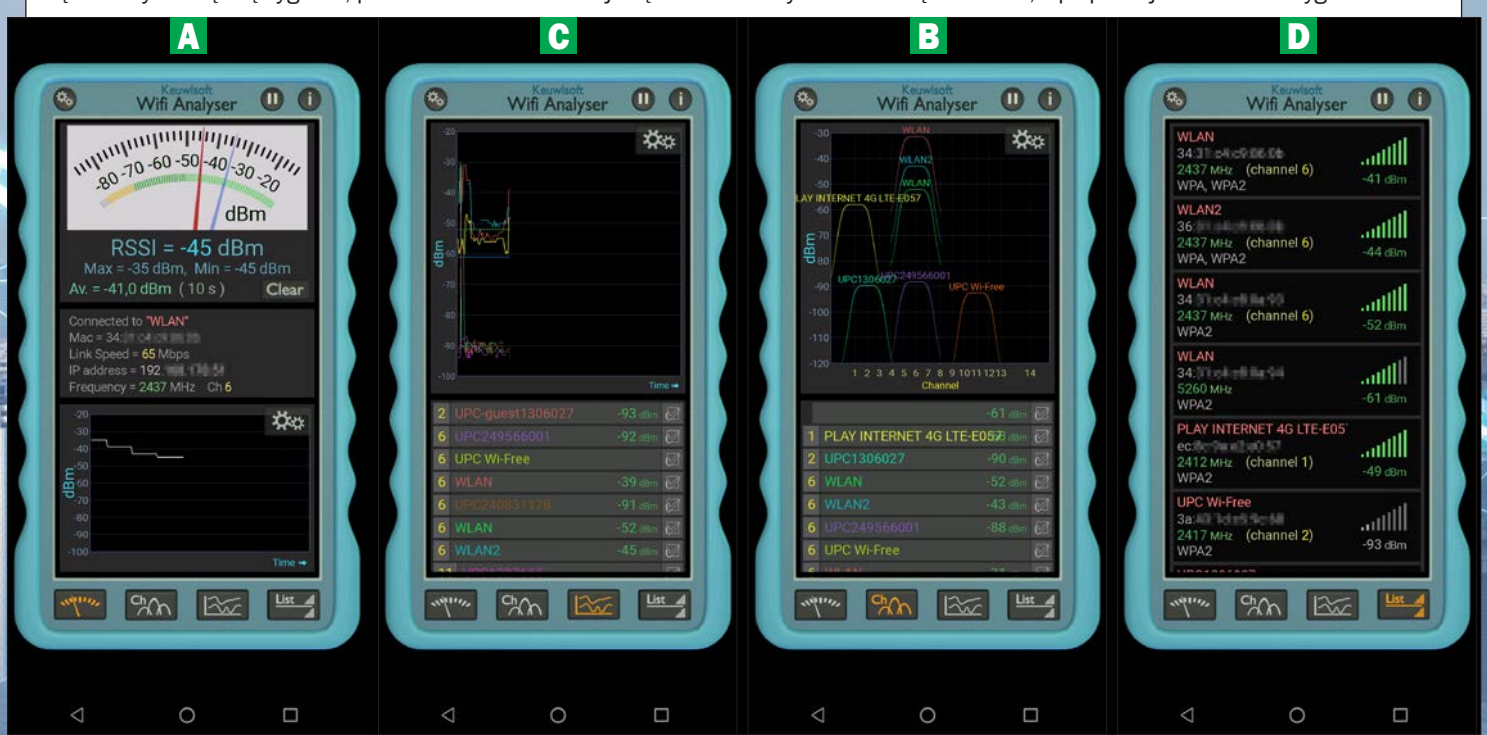
Wifi Analyser to narzędzie mobilne do łatwej diagnostyki sieci Wi-Fi. W przeciwieństwie do poprzedniej aplikacji, ten program lepiej nadaje się do szybkiego zmierzenia siły sygnału naszej sieci, a nie do sprawdzenia wszystkich sieci w okolicy.

1 Po uruchomieniu aplikacji zobaczymy interfejs stylizowany na miernik sygnału **A**. Na bieżąco, gdy chodzimy ze smartfonem po domu, aplikacja mierzy siłę sygnału naszej sieci Wi-Fi (tej, z którą smartfon jest w danym momencie połączony). Podaje też minimalną i maksymalną siłę sygnału, pomiar średni (z ostatnich 10 sekund) i takie parametry, jak szybkość połączenia, adres MAC, adres IP, częstotliwość (pasmo) i kanał. W dolnej części ekranu kreślony jest na bieżąco wykres siły sygnału naszej sieci. Dostęp do pozostałych funkcji aplikacji uzyskujemy za pośrednictwem czterech ikon rozmieszczonych wzdłuż dolnej krawędzi ekranu.

2 Wskazanie drugiej z czterech ikon **B** funkcyjnych aplikacji powoduje wyświetlenie wykresu siły sygnału wykrytych sieci Wi-Fi oraz kanałów, w jakich te sieci pracują. W dolnej części ekranu wymienione są nazwy wykrytych sieci. Możemy łatwo usuwać z wykresu niepotrzebne dane, usuwając zaznaczenia z pól wyboru po prawej stronie.

3 Aplikacja może też tworzyć w czasie rzeczywistym wykres mocy sygnału różnych sieci w okolicy **C**. Możemy usuwać z wykresu sieci, zostawiając tylko te, które nas interesują.

4 Ostatni ekran aplikacji pokazuje listę parametrów wykrytych sieci Wi-Fi **D**: nazwy sieci, adresy MAC ruterów/punktów dostępowych, pasma (częstotliwości), kanały i typy szyfrowania, a po prawej stronie – siła sygnału. **as**



* Kod QR szybko przenosi na stronę, skąd można pobrać aplikację. Skanujemy go smartfonem za pomocą dowolnej aplikacji QR pobranej z Google Play

TRIKI
DO INTERNETU
LEPSZE WI-FI

SPOSOBÓW
JAK POPRAWIĆ DZIAŁANIE WI-FI W DOMU

Jeśli irytuje nas działanie Wi-Fi w domu, najwyższa pora je poprawić. Często ***nie wymaga to wcale wiele zachodu****. Oto kilka pomysłów i sposobów, jak usprawnić działanie sieci bezprzewodowej. Warto je wypróbować*

Każda osoba korzystająca z sieci Wi-Fi natrafiła kiedyś na problem słabego zasięgu. Najgorzej, jeżeli spotykamy się z nim we własnym domu lub mieszkaniu. Istnieje jednak kilka sposobów na poprawienie działania naszej sieci, a część z nich możemy wypróbować niemal od razu, bez wydawania jakichkolwiek pieniędzy na dodatkowy sprzęt. Poznajmy osiem skutecznych sposobów na poprawienie działania domowej sieci bezprzewodowej. **bs**

1 ODPOWIEDNIE POŁOŻENIE RUTERA

Właściwe umiejscowienie rutera w domu to sprawa kluczowa, o której wielu użytkowników wciąż zapomina. Główna zasada jest prosta – **ruter powinien stać możliwie najbliżej centralnego miejsca naszego domu**. Jako że sygnał rozchodzi się naokoło urządzenia, ustawienie go przy zewnętrznej ścianie mieszkania lub budynku będzie dużym marnotrawieniem jego mocy, o ile nie zależy nam na zasięgu Wi-Fi na przykład w przydomowym ogródku. Ruter nie powinien również stać na podłodze – najlepiej umieścić go na jakimś meblu, co usprawni rozchodzenie się fal. Trzeba jednak pamiętać, że wpływ na rozchodzenie się sygnału ma sporo czynników. Najbardziej oczywistym są ściany, okna i drzwi. Ich liczba, grubość, a nawet materiały, z jakich są wykonane, mają wpływ na to, jak silny sygnał z rutera odbierzemy po ich drugiej stronie. Należy też zadbać, aby w pobliżu nie znajdowały się inne urządzenia elektryczne (telewizor, mikrofalówka itp.) ani duże metalowe obiekty, jak chociażby kaloryfery. Wpływają one negatywnie na jakość sygnału i mogą spowodować, że nawet z niewielkiej odległości nie uzyskamy pełnej przepustowości naszego łącza internetowego.

Jakość sygnału w różnych miejscach naszego domu możemy zmierzyć sami za pomocą smartfona. Istnieje wiele aplikacji pokazujących w czasie rzeczywistym siłę sygnału Wi-Fi. Jednym z najpopularniejszych jest darmowy **Wi-Fi Analyzer** na smartfony z Androidem, który znajdziemy w Sklepie Play. W głównym oknie programu od razu po uruchomieniu wyświetlają się statystyki wszystkich sieci, których sygnał dociera do naszego smartfona. Wystarczy teraz odnaleźć wśród nich nazwę naszej sieci, a następnie przejść się po wszystkich pomieszczeniach, by sprawdzić, jak silny sygnał tam dociera. Jeżeli zauważymy wysokie spadki, będziemy mogli korygować umiejscowienie rutera, aż osiągniemy optymalny rezultat.

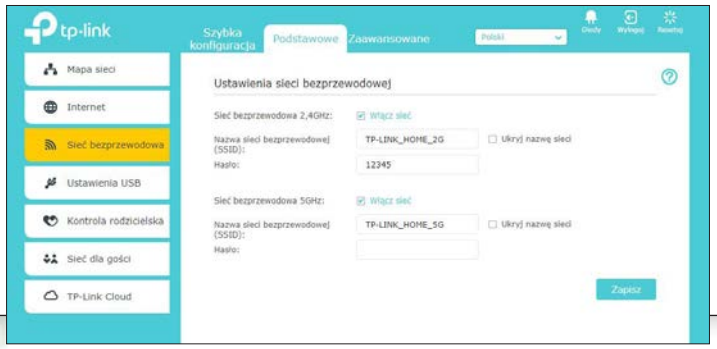
2 USTAWIENIE ANTENY W RUTERZE

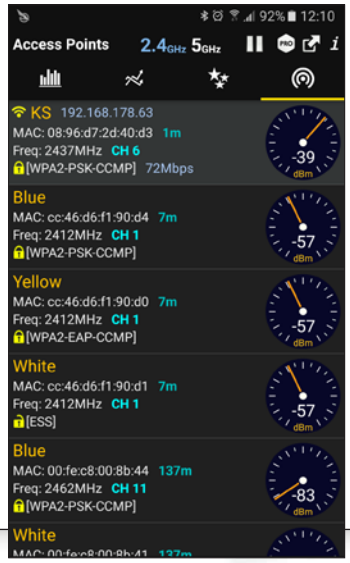
Najczęściej spotykane w ruterach są niewielkie anteny dookólne, które rozsyłają sygnał na boki. W praktyce oznacza to, że najlepszy zasięg w jednej kondygnacji otrzymamy po ustawieniu anteny pionowo. Co jednak w sytuacji, gdy jednym ruterem chcemy pokryć kilka kondygnacji naszego domu? **Jednym z rozwiązań jest zamontowanie w ruterze (o ile to możliwe) dwóch anten**, a następnie ustawienie jednej w pionie, a drugiej poziomo, co pozwoli na przesłanie silniejszego sygnału w górę i w dół.

3 ZMIANA CZĘSTOTLIWOŚCI SIECI BEZPRZEWODOWEJ

Wszystkie urządzenia korzystające z bezprzewodowej łączności Wi-Fi pracują na częstotliwości 2,4 GHz. Powoduje to, że przy dużej liczbie urządzeń i sieci sygnały mogą się wzajemnie zakłócać. Na tej samej częstotliwości pracują też między innymi mikrofalówki czy zdalnie sterowane zabawki. Sporo urządzeń wspiera już jednak łączność na częstotliwości 5 GHz, która jest zwykle znacznie mniej oblegana, a co za tym idzie – zakłócenia w jej obrębie są znacznie mniejsze.

Jeżeli nasz ruter obsługuje zarówno częstotliwość 2,4 GHz, jak i 5 GHz, możemy w panelu administratora urządzenia aktywować obie wartości albo pozostawić tylko wyższą. W tym drugim wypadku trzeba jednak upewnić się, że wszystkie urządzenia, z których korzystamy, mogą działać na częstotliwości 5 GHz, inaczej łączność z nimi będzie niemożliwa. Opcja ustawień pasma dostępna jest zwykle w zakładce **Sieć bezprzewodowa (wireless)**. Opis, jak wejść do panelu administratora rutera, znajdziecie w jego instrukcji obsługi. Najczęściej jednak dostaniemy się do niego, wpisując w pasku adresu przeglądarki adres **192.168.0.1** lub **192.168.1.1**, a następnie logując się na wyświetlonej stronie. W razie problemów z dostępem do panelu należy skontaktować się z dostawcą usług internetowych. Trzeba jednak pamiętać, że używając częstotliwości 5 GHz, zmniejszamy realny zasięg naszej sieci z około 70 do około 35 metrów wewnątrz budynku. Najczęściej jednak taki zasięg będzie wystarczający przy umieszczeniu rutera w optymalnym miejscu, a zmniejszenie zakłóceń zrekompensuje zmniejszenie zasięgu.

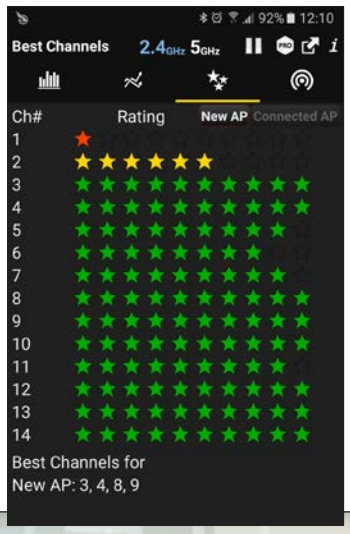


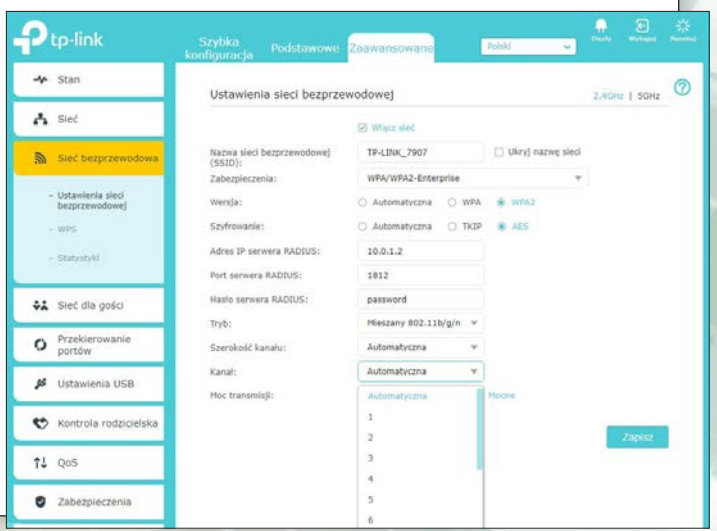


4 OPUSZCZENIE ZATŁOCZONEGO KANAŁU

Jeżeli przejście na częstotliwość 5 GHz jest dla nas z jakiegoś powodu niemożliwe, mamy jeszcze inną możliwość zwalczenia zbyt wielu zakłóceń. Mowa o **wybraniu innego kanału transmisji**. Domyślnie ruter przy pierwszej konfiguracji sam dopasowuje kanał, z którego będzie korzystał. W paśmie 2,4 GHz część kanałów jednak nachodzi na siebie, dlatego też warto wybrać taki, który znajduje się możliwie najdalej od tych używanych przez najwięcej urządzeń wokół nas (najczęściej to kanały 1 i 6).

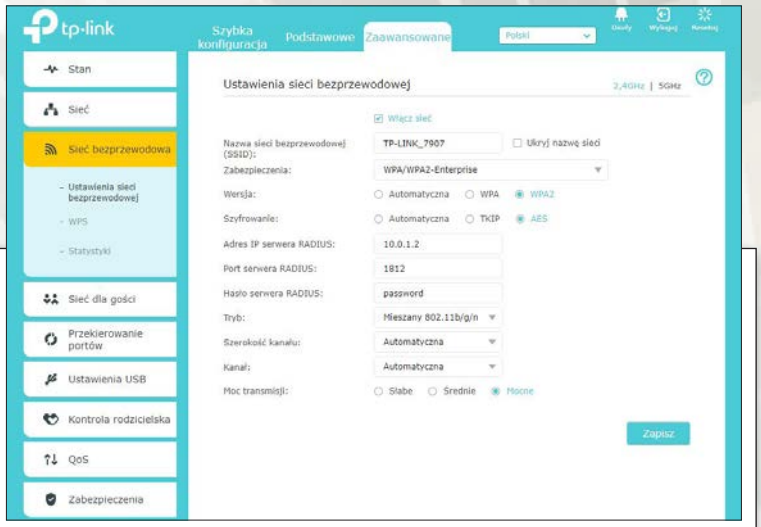
Do sprawdzenia, które kanały są najbardziej zatłoczone, posłuży wspominany już wyżej mobilny program **Wi-Fi Analyzer**. Wykres na głównym ekranie pokazuje rozmieszczenie konkretnych sieci na kanałach od 1 do 14 (poziomą oś). W trzeciej zakładce, nazwanej Best Channels, znajdziemy informacje o tym, które kanały oferują najmniejsze zakłócenia. Aplikacja sama też sugeruje, na które z nich najlepiej jest się przenieść w danej lokalizacji – informacja o tym znajduje się na dole ekranu. Po wybraniu optymalnego kanału należy zmienić go w ustawieniach rutera. W tym celu ponownie wchodzimy do panelu administracyjnego i znajdujemy zakładkę odpowiedzialną za ustawienia sieci bezprzewodowej. Zmiana kanału w wielu urządzeniach będzie wymagała przejścia do ustawień zaawansowanych. W każdym przypadku musimy jednak szukać opcji oznaczonej po prostu jako **kanał (channel)**. Następnie z rozwijalnej listy wybieramy odpowiednią wartość. Po restarcie rutera nasza sieć będzie działała z nowymi ustawieniami.





Fot. Helenstock/123rf.com

5 MOC RUTERA

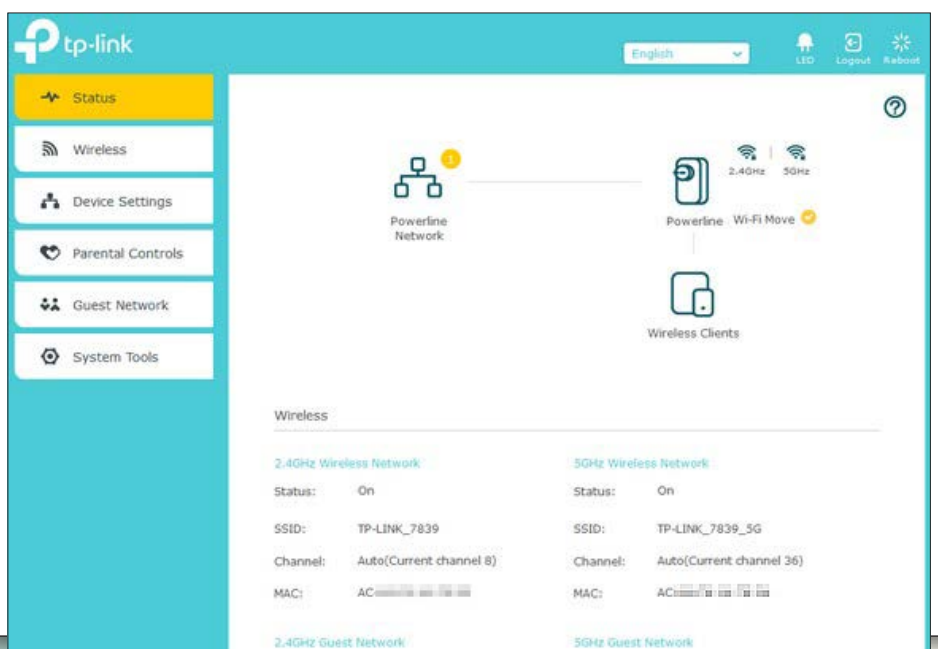


Część ruterów umożliwia **ustawienie mocy.** W zależności od producenta i modelu domyślnie ustawioną wartością może nie być ta najwyższa. Maksymalna możliwa moc, jakiej możemy używać w Polsce, to 100 mW dla częstotliwości 2,4 GHz. Jeżeli nasz ruter umożliwia ustawienie mocy, znajdziemy tę opcję najczęściej w ustawieniach zaawansowanych w panelu administratora. Może ona mieć wartości procentowe, określone w miliwatach, lub – jak w naszym przykładzie – trzy stopnie oznaczone jako **słabe**, **średnie** i **mocne**. Im wyższa moc, tym zasięg sieci jest większy.

6 INTERNET Z GNIAZDKA ELEKTRYCZNEGO

Jeśli omówione na stronie obok repeatery nie dają nam satysfakcjonujących rezultatów (może tak być w przypadku budynków z grubymi, zbrojonymi ścianami, gdzie sygnał traci na jakości już po kilku metrach), najprostszym rozwiązaniem byłoby oczywiście położenie kabla Ethernet, jednak jest to dość kłopotliwe i często wymaga wiercenia w ścianach. Alternatywą jest tu **Powerline, a więc sieć internetowa rozprzestrzeniana za pomocą domowej sieci elektrycznej.** Powerline działa w kilku standardach. Nowsze oferują większą przepustowość, ale są też zauważalnie droższe. Warto zainwestować w urządzenia odpowiadające transferowi oferowanemu przez dostawcę internetu.

Instalacja Powerline jest niezwykle prosta. W skład standardowego zestawu wchodzą co najmniej dwa adaptery. Jeden z nich wpinamy do gniazdka elektrycznego w okolicy rutera, a następnie łączymy z nim za pomocą kabla Ethernet bądź bezprzewodowo, jeżeli adapter na to pozwala. Od tego momentu sygnał internetowy będzie dostępny w każdym gniazdku w obrębie jednego licznika elektrycznego i jednej fazy – trzeba więc zawczasu upewnić się, czy na przykład w naszym domu wszystkie kondygnacje mają tę samą fazę. W przeciwnym wypadku może się okazać, że Powerline po prostu nie zadziała. Drugi adapter podłączamy z kolei w miejscu, gdzie chcemy doprowadzić sygnał – możemy go wyprowadzić kablem bądź – w przypadku wielu modeli – także bezprzewodowo. Trzeba mieć jednak na uwadze, że na Powerline również wpływają czynniki zewnętrzne osłabiające jakość sygnału. To między innymi wiek instalacji elektrycznej, a także liczba urządzeń do niej podłączonych. Straty nie powinny być jednak na tyle duże, by Powerline traktować jako ostateczność.



7 POSZERZENIE ZASIĘGU REPEATEREM

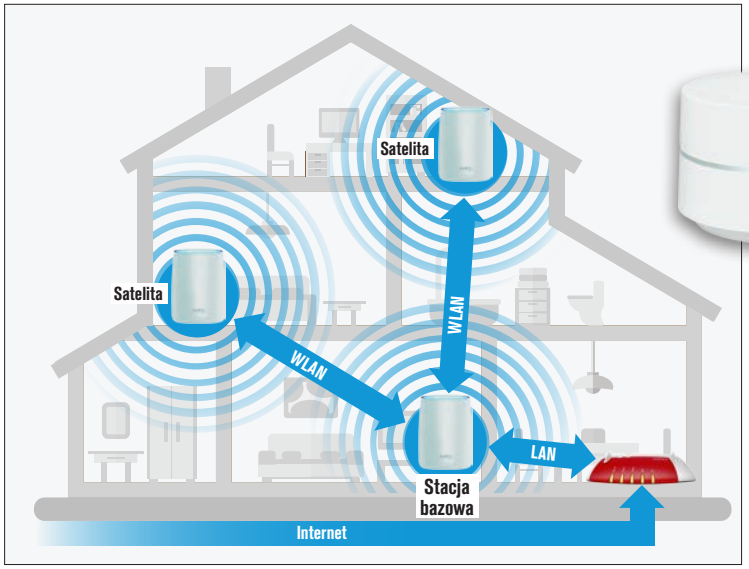
To także płatne rozwiązanie. Warto postawić właśnie na nie, jeśli wyczerpały się możliwości bezpłatnego poprawienia działania sieci Wi-Fi, a wciąż mamy problemy z zasięgiem. **Repeatery to urządzenia, które odbierają sygnał z rutera, regenerują go, a następnie emitują dalej odpowiednio wzmocniony.**

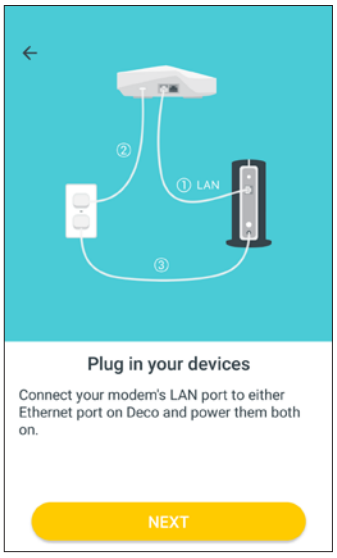
Repeater jest bardzo skutecznym urządzeniem do pokrywania większych obszarów sygnałem Wi-Fi, ale należy pamiętać o jego właściwym rozmieszczeniu. Urządzenie to nie powinno znajdować się za blisko rutera – wtedy zasięg nie zostanie odpowiednio wzmocniony. Nie należy umieszczać go również w miejscach o słabym zasięgu – wtedy repeater odbierze sygnał z zakłóceniami i taki sam będzie przekazywał dalej. Optymalnie powinniśmy zainstalować to urządzenie w połowie dystansu pomiędzy ruterem a urządzeniem, które ma odbierać sygnał. Zapewni to balans pomiędzy pokryciem jak największego obszaru a jakością wzmacnianego sygnału. Instalacja repeatera nie jest skomplikowana i zwykle łatwo opisana w instrukcji obsługi.

W zależności od producenta i modelu możemy skorzystać z funkcji WPS bądź skonfigurować go z poziomu przeglądarki. Domyślnie repeatery widoczne są przez nasze urządzenia tak samo jak ruter. Część modeli ma jednak możliwość ustawienia indywidualnej nazwy i hasła.

8 SIECI MESH – WI-FI NOWEJ GENERACJI

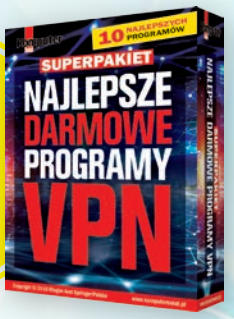
Wi-Fi mesh (z angielskiego siatka) to sieć niewielkich stacji Wi-Fi połączonych w jeden inteligentny system, który automatycznie wykrywa sygnał sieci i przekazuje go dalej, pokrywając sygnałem znacznie większy obszar niż pojedynczy ruter. Całość działa na podobnej zasadzie jak repeatery, poza tym, że wszystkie elementy systemu, poza stacją bazową, którą podłączamy do modemu lub gniazda sieci LAN, nie wymagają żadnej ingerencji z naszej strony. Automatycznie wykrywają sygnał z okolicznych nadajników i przesyłają go dalej. To świetne rozwiązanie, jeżeli chcemy mieć pewność, że sygnał będzie bardzo dobry w każdym zakątku mieszkania czy nawet dużego, wielopiętrowego domu. Ważną cechą sieci mesh jest ich prosta konfiguracja i bezproblemowe użytkowanie. W przeciwieństwie do repeaterów, sieci mesh można konfigurować z poziomu aplikacji w smartfonie, który ze stacją bazową łączy się za pomocą Blue tooth. Kiedy skończymy proces konfiguracji, to gdy będziemy chodzić po domu na przykład ze smartfonem, urządzenie automatycznie będzie odbierało sygnał z najbliższego nadajnika w taki sposób, że nie powinniśmy odczuć momentu, w którym następuje przełączenie. W przypadku zwykłego repeatera może dojść do sytuacji, w której smartfon lub laptop będą podłączone do odległego rutera, dopóki sami nie wybierzemy innego źródła sygnału. Natomiast gdy okaże się, że gdzieś w domu nie ma dobrego zasięgu, wystarczy dokupić satelitę – w przypadku niektórych producentów możemy stworzyć sieć nawet dziewięciu urządzeń. (Więcej o Wi-Fi mesh przeczytamy w Komputer Świecie 7/2018, dostępnym w KŚ+ – www.kslpus.pl).





TRIKI
DO INTERNETU
JAK KORZYSTAĆ Z VPN

ANONIMOWE I



NA NASZEJ PŁYCIE DVD ***PAKIET 10 PROGRAMÓW*** *DO VPN*

Wirtualna sieć prywatna, czyli VPN, pozwala na utworzenie specjalnego tunelu pomiędzy dwoma punktami w publicznej sieci. ***Przesyłane w ten sposób dane są całkowicie bezpieczne i najczęściej mocno zabezpieczone.*** *Z poradnika Komputer Świata dowiemy się, jak sprawnie korzystać z VPN*

VPN to skrót od Virtual Private Network (Wirtualna Sieć Prywatna). Połączenia między dwoma punktami wewnątrz takiej sieci nazywamy tunelowymi ze względu na to, że są zaszyfrowane i nie da się ich „podsłuchać". Możemy porównać takie łącze do tunelu utworzonego między tymi punktami w internecie.

Dlaczego warto korzystać z sieci VPN

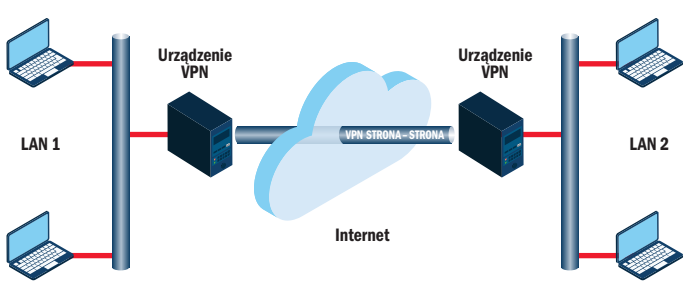
Sieci VPN często są wykorzystywane w firmach, gdzie bezpieczeństwo danych jest priorytetem. Pracownik, korzystając z takiej sieci, może zdalnie uzyskiwać dostęp do zasobów na serwerach firmy, a nikt inny nie może sprawdzić i podejrzeć pakietów, jakie są przesyłane. Jednak również użytkownicy domowi coraz częściej zaczynają przywiązywać większą wagę do bezpieczeństwa i anonimowości w sieci. Nie chcemy, aby ktoś mógł podejrzeć, jakie strony w sieci odwiedzamy, jakie dane logowania podajemy na niezabezpieczonych witrynach, co pobieramy z internetu na dysk. Dbanie o prywatność jest szczególnie ważne w przypadku, gdy korzystamy z otwartych punktów dostępowych (hotspotów), na przykład na lotnisku czy w kawiarni albo w galerii handlowej – nigdy wtedy nie możemy mieć pewności, czy ktoś nie śledzi i nie sprawdza wszystkich pakietów sieciowych w poszukiwaniu haseł lub innych wrażliwych informacji.

VPN zabezpiecza nas przed każdym możliwym rodzajem ataku wewnątrz sieci lokalnej, dlatego też warto korzystać z takiego rodzaju połączenia jak najczęściej, a szczególnie w miejscach podwyższonego ryzyka. **kd**

WARTO WIEDZIEĆ

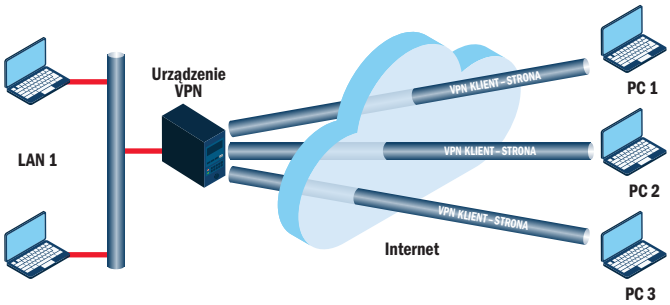
Jeśli korzystamy z programów do zdalnej kontroli pulpitu, jak na przykład **TeamViewer**, to również korzystamy z połączenia VPN. Połączenie to jest realizowane pomiędzy dwoma komputerami w sieci, a wymiana danych pomiędzy nimi jest zabezpieczona i zaszyfrowana. Jest to najprostszy rodzaj sieci VPN.

TYPY SIECI VPN



STRONA–STRONA (Site–Site)

Kanał VPN zestawiany między dwoma, odległymi fizycznie, sieciami LAN. Urządzeniem VPN może być serwer firmowy lub odpowiednio skonfigurowany ruter z obsługą sieci VPN. To rozwiązanie jest przeważnie wykorzystywane w firmach, gdyż zapewnia możliwość dostępu do wewnętrznej sieci LAN, na przykład między różnymi oddziałami firmy.



KLIENT–STRONA (Client–Site lub Gateway)

Jest to kanał VPN zestawiany pomiędzy odległą fizycznie siecią LAN a urządzeniem klienta. Sieć LAN może należeć na przykład do firmy, a rolę „bramy" może pełnić serwer lub odpowiednio skonfigurowany ruter. Jest to idealne rozwiązanie w przypadku, gdy chcemy na przykład mieć dostęp do firmowej sieci z dowolnego miejsca na świecie. Dzięki niemu połączymy się szyfrowanym połączeniem VPN i będziemy mogli bezpiecznie pracować na firmowych zasobach.

BEZPIECZNE PRZEGLĄDANIE INTERNETU

RODZAJE PROTOKOŁÓW

Protokoły sieci VPN to inaczej protokoły komunikacyjne z określonymi regułami i zasadami, które mają pozwolić na bezpieczne połączenia pomiędzy dwoma punktami. Oto najpopularniejsze protokoły sieci VPN

PPTP

Jeśli korzystamy z tego typu protokołu, powinniśmy jak najszybciej przestać. Ma on kilka zalet, ale brak bezpieczeństwa całkowicie przekreśla jego przydatność, a Microsoft odradza jego używanie. Niestety, nadal jest stosowany przez wiele firm i użytkowników nieświadomych potencjalnego zagrożenia.

Zalety:
- szybkie działanie, prostota nie wpływa na wydajność
- łatwa konfiguracja
- dostępny praktycznie na każdym urządzeniu

Wady:
- nawet silnie zabezpieczona sesja może być złamana w ciągu 24 godzin
- brak mocnego szyfrowania

L2TP/IPSec

Jest to hybryda dwóch protokołów, samo L2TP pozwala tylko na utworzenie tunelu komunikacyjnego i przesyłanie danych. Za bezpieczeństwo odpowiedzialny jest protokół IPSec, który uwierzytelnia i szyfruje połączenia. Zapewniał wysokie bezpieczeństwo, jednak po ujawnieniu przez Edwarda Snowdena informacji o NSA można przyjąć, że protokół IPSec nie zapewnia wcale tak wysokiej ochrony i może być złamany przez służby specjalne.

Zalety:
- szybkość działania
- wysokie bezpieczeństwo
- powszechnie dostępny wróżnych systemach

Wady:
- istnieje wysokie ryzyko złamania szyfrowania IPSec przez NSA, co może stanowić zagrożenie
- działa na porcie UDP 500, przez co łatwo wykryć korzystanie z sieci VPN, a niektórzy usługodawcy internetu i hotspoty blokują ten port

OpenVPN

Hybryda różnych protokołów, która zapewnia najwyższy stopień ochrony. Nie ma żadnych doniesień, które sugerowałyby złamanie jej zabezpieczeń. Wykorzystuje bibliotekę OpenSSL i protokoły SSLv3 oraz TLSv1. Pozwala to na korzystanie z najlepszych form szyfrowania połączenia i zabezpieczania sesji. Można też łączyć się za pomocą dowolnego portu, dzięki czemu unikniemy wykrycia, że korzystamy z połączenia z siecią VPN.

Zalety:
- otwarty kod źródłowy
- najwyższy poziom bezpieczeństwa
- szerokie możliwości konfiguracji

Wady:
- wymaga instalacji specjalnej aplikacji
- konfiguracja może sprawić trudność początkującym użytkownikom

SZYBKOŚĆ POBIERANIA PRZEZ VPN

Podczas korzystania z internetu przez VPN strony wczytują się wolniej, ponieważ nasze pakiety muszą przebyć czasami bardzo długą drogę, zanim trafią do odpowiedniego serwera. W zależności od tego, jaki program wybierzemy, możemy spodziewać się różnych szybkości transferu. Komputer Świat sprawdził pod tym kątem opisywane w tym wydaniu programy.

Testowe łącze bez szyfrowanego połączenia osiąga maksymalnie około 120 Mb/s. Najgorszy w zestawieniu **Speedify** (DVD-KOD: **055**) z szybkością 2,12 Mb/s pozwala jedynie na powolne przeglądanie stron internetowych. Zdecydowanie na wyróżnienie zasłużyły **Windscribe VPN** (DVD-KOD: **066**) oraz **PrivateTunnel** (DVD-KOD: **046**), które bez problemu poradzą sobie nawet ze streamowaniem wysokiej jakości filmów. Do testowania wykorzystano stronę **www.speedtest.net** i optymalne ustawienia w każdym programie (automatyczny wybór serwera, a jeśli takiej opcji nie było, wybierano najbliższy dostępny darmowy serwer).

SZYBKOŚĆ POBIERANIA DLA OPISYWANYCH VPN-ÓW

Nazwa	Ping [ms]	Pobieranie [Mb/s]	Wysyłanie [Mb/s]
Bez VPN	2	119,53	12,13
Windscribe VPN	25	108,15	11,39
PrivateTunnel	23	94,07	11,81
ProtonVPN	31	75,38	11,82
Hotspot Shield	60	58,91	12,28
hide.me	49	56,19	11,93
TunnelBear	30	33,83	10,62
SurfEasy	41	31,39	11,87
CyberGhost	52	23,83	11,79
Avira Phantom VPN	25	19,25	11,09
OpenVPN	40	13,65	4,26
Speedify	62	2,12	0,53

SZYFROWANIE

Każde połączenie VPN jest odpowiednio szyfrowane, właśnie dzięki temu nie można „podsłuchać" naszego ruchu sieciowego. Najlepsze serwery korzystają z nowoczesnych zabezpieczeń, których nie da się złamać. Dobrym przykładem jest opisywany dalej serwer **OpenVPN**, który korzysta z szyfrowania **AES-256-CBC**. Jest to symetryczny szyfr blokowy o długości klucza 256 bit, z systemem CBC (Cipher Block Chaining), co oznacza, że każda wiadomość jest zależna od poprzedniej. Szyfrowanie tego typu jest wykorzystywane między innymi przez agencję NSA do ochrony ściśle tajnych dokumentów. Uważa się, że jest nie do złamania.

Fot. Nikita Gonin/123rf.com

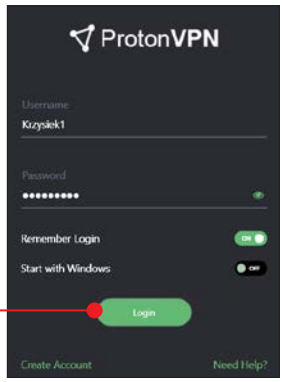
ŁATWE ROZWIĄZANIA DLA KAŻDEGO

VPN DLA KAŻDEGO: PROTONVPN

ProtonVPN (DVD-KOD: **048**) to darmowy VPN od twórców bezpiecznej poczty ProtonMail, pozwalający ukryć naszą lokalizację i ominąć blokady regionalne w serwisach internetowych, których zasięg został ograniczony do wybranych krajów. W podstawowej, bezpłatnej wersji można korzystać tylko z trzech lokalizacji. Przy pierwszym uruchomieniu programu można aktywować darmowy, 7-dniowy okres próbny konta Plus. Po upływie tego czasu konto przełączy się do uproszczonej, bezpłatnej wersji. Zanim zaczniemy korzystać z programu, będziemy musieli założyć darmowe konto.

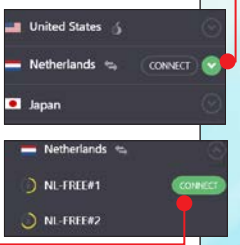
Wybieramy serwer

Zamiast decydować się na automatyczne nawiązanie połączenia, lepiej samemu wskazać serwer znajdujący się najbliżej nas. Różnice w szybkości wczytywania stron mogą być ogromne, dlatego warto poświęcić chwilę na dokonanie odpowiedniego wyboru.



1 Logujemy się do ProtonVPN, a po zalogowaniu się klikamy na zakładkę **Countries**.

2 Poniżej znajdziemy listę dostępnych państw. Wybieramy państwo, które jest najbliżej, i klikamy na strzałkę po jego prawej stronie.



3 Po rozwinięciu listy będziemy mogli sprawdzić obciążenie serwerów i ich dostępność – wybierajmy jak najmniej obciążone serwery, klikając na przycisk **Connect**.

ProtonVPN
internet https://protonvpn.com
system Windows XP, Vista, 7, 8, 10
język angielski
ograniczenia brak
rejestracja niewymagana

Plusy i minusy:
- darmowy okres próbny konta Plus
- wsparcie sieci Tor
- możliwość wyboru serwera

ŁATWY W OBSŁUDZE: CYBERGHOST VPN

CyberGhost VPN (DVD-KOD: **048**) – popularny program do anonimowego korzystania z internetu. Można sprawdzić jego działanie, korzystając z jednodniowego okresu próbnego, podczas którego dostępne są wszystkie opcje pełnej wersji. CyberGhost łączy się z zewnętrznym serwerem VPN, przez który będziemy korzystać z sieci – dane wysyłane i odbierane przez nasz komputer zostaną zaszyfrowane, a odwiedzane strony nie będą miały dostępu do naszego adresu IP (będą mogły odczytać jedynie adres serwera VPN), umożliwiając również omijanie blokad regionalnych w niektórych serwisach. Wymagane jest założenie konta.

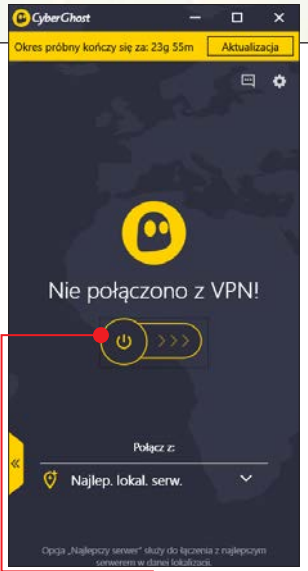
CyberGhost VPN
internet www.cyberghostvpn.com
system Windows XP, Vista, 7, 8, 10
język polski
ograniczenia wersja trial działa jeden dzień
rejestracja niewymagana

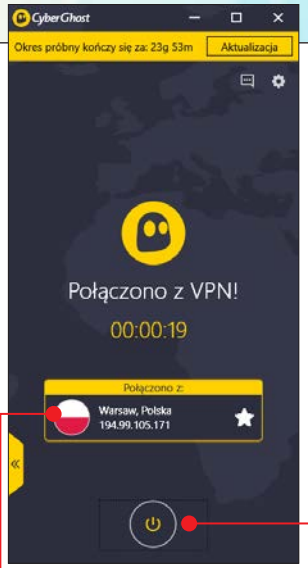
Plusy i minusy:
- różne tryby pracy
- możliwość wyboru serwera
- mocny algorytm szyfrujący

Korzystamy z VPN

1 Po uruchomieniu programu klikamy na ikonę kółka zębatego, a następnie na **Settings**.

2 Klikamy na liście przy opcji **Language**, wybieramy z listy opcję **Polish** i klikamy na **Apply**. Program zostanie uruchomiony ponownie.





3 Teraz wystarczy, że klikniemy na przycisk włączania na środku okna, a zostanie nawiązane połączenie z najlepszym dla nas serwerem. Możemy też sami wybrać serwer.

4 W celu przerwania połączenia też klikamy na przycisk.

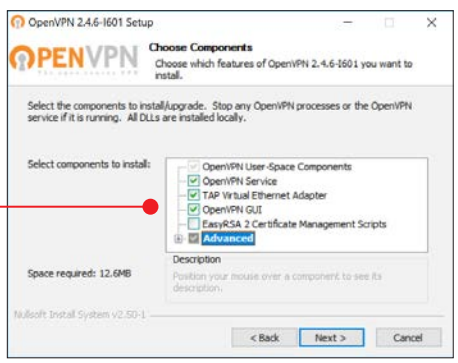
ROZWIĄZANIE DLA ZAAWANSOWANYCH

ZAPEWNIA NAJWIĘKSZE MOŻLIWOŚCI: OPENVPN

OpenVPN (DVD-KOD: **040**) – ceniony, wieloplatformowy i otwartoźródłowy pakiet oprogramowania do tworzenia zaszyfrowanych połączeń między hostem a komputerem lokalnym przez internet. OpenVPN oferuje kilka metod uwierzytelnienia użytkowników: poprzez klucze, certyfikaty lub nazwę użytkownika i hasło. Aplikacja pozwala również na obsługę dynamicznych adresów IP. Jej konfiguracja nie należy do najprostszych, jednak gdy przez nią przejdziemy, będziemy mogli cieszyć się bezpiecznym połączeniem bez zbędnych reklam i kolejek, a za to z dostępem do ogromnej liczby serwerów na całym świecie.

Konfigurujemy program do pracy

Podczas instalacji zaleca się zachować domyślne ustawienia i wyrazić zgodę na instalację wszystkich dodatkowych składników – w innym wypadku program może nie działać prawidłowo.

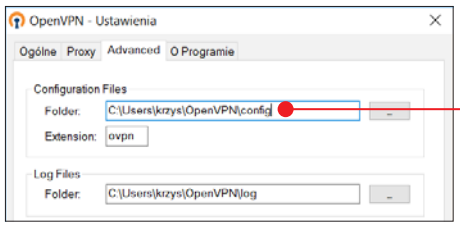


Następnie musimy dodać specjalne pliki konfiguracyjne, które pozwolą na łączenie się z wybranym serwerem VPN. Oto jak to zrobić.

1 Uruchamiamy OpenVPN GUI.

2 Następnie klikamy prawym przyciskiem myszy na ikonę w zasobniku systemowym, a później na **Ustawienia**.

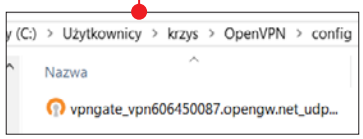
3 Przechodzimy do zakładki **Advanced** i sprawdzamy lokalizację folderu, w którym są pliki konfiguracyjne. Otwieramy Eksplorator i nawigujemy do tej lokalizacji.



4 Za pomocą przeglądarki wchodzimy na adres **https://www.vpngate.net/en**, możemy też skorzystać z innych stron oferujących darmowy lub płatny dostęp do serwerów VPN. Na liście serwerów w kolumnie **OpenVPN** **A** klikamy na **OpenVPN Config file** **B**.

5 Następnie klikamy na link z napisem OpenVPN i zapisujemy plik konfiguracyjny na naszym dysku.

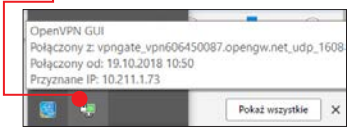
6 Przenosimy pobrany plik do folderu konfiguracyjnego (patrz punkt **3**).



7 Teraz zamykamy i ponownie uruchamiamy program OpenVPN. Po kliknięciu na jego ikonę zobaczymy cztery serwery, z którymi możemy nawiązać połączenie. Wystarczy najechać kursorem na jeden z nich, a następnie kliknąć na **Połącz**.

8 Pojawi się okno z prośbą o podanie loginu i hasła, dla serwerów z podanej wyżej strony domyślny login to **vpn**, a hasło to **vpn**. Zaznaczamy opcję **Save password** i klikamy na **OK**.

9 Po poprawnym zestawieniu połączenia ikona klienta OpenVPN zmieni kolor na zielony.



10 Po sprawdzeniu naszego adresu IP po zestawieniu połączenia okaże się, że łączymy się szyfrowanym połączeniem z innego kraju niż nasz.

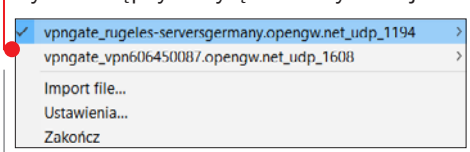
Automatyczny start

1 Klikamy prawym przyciskiem myszy na ikonę programu w zasobniku systemowym i wybieramy opcję **Ustawienia**.

2 Następnie zaznaczamy opcję **Launch on Windows startup**.

Szybka zmiana serwera

Jeśli pobierzemy i dodamy do folderu konfiguracyjnego wiele plików, będziemy mogli bardzo szybko przechodzić między różnymi serwerami. Warto dodać różne serwery na przykład z USA, Niemiec, Francji itp., dzięki temu będziemy mogli uzyskać dostęp do danych dostępnych wyłącznie w tych krajach.

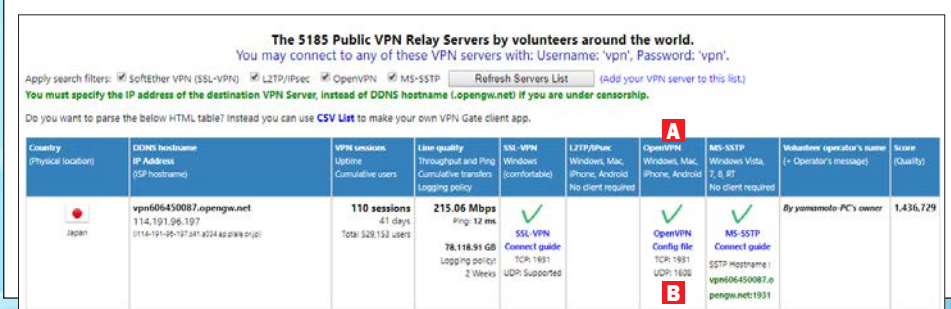


OpenVPN

internet https://openvpn.net
system Windows XP, Vista, 7, 8, 10
język polski
ograniczenia brak
rejestracja niewymagana

Plusy i minusy:

- skomplikowana konfiguracja
- często zmieniane hasła do serwerów
- dość wolne połączenie zależne od serwera
- brak limitu danych transferowych

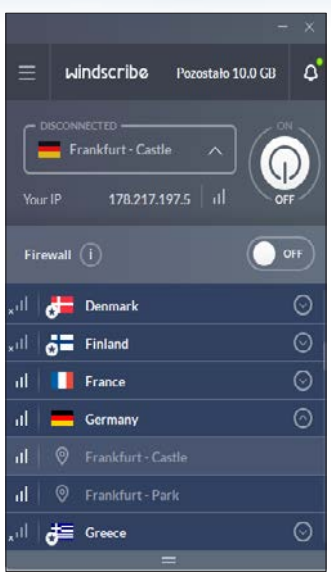


TRIKI
DO INTERNETU
SUPERPAKIET VPN

8 NAJCIEKAWSZYCH PROGRAMÓW DO

VPN-y zapewniają prywatność w internecie. A możliwość ***ochrony prywatności i lokalizacji jest kluczowa dla wielu użytkowników****. W superpakiecie na płycie dołączonej do tego wydania znajdziemy najciekawsze programy, które pozwolą nam cieszyć się darmowym bezpiecznym łączem*

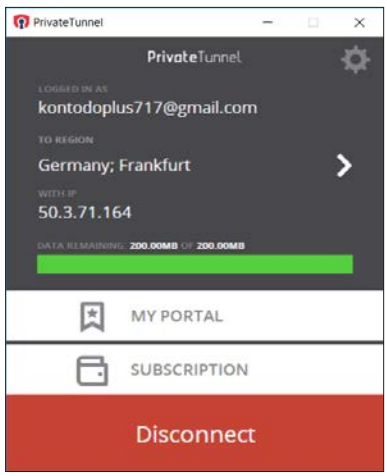
WINDSCRIBE VPN



Program do anonimowego korzystania z internetu. Windscribe ukrywa naszą lokalizację, szyfruje ruch w trakcie przeglądania, blokuje reklamy, pozwala również ominąć blokady regionalne. Darmowa wersja programu daje dostęp do serwerów VPN w 10 lokalizacjach (między innymi USA, Kanada, Wielka Brytania, Hongkong, Francja, Niemcy, Holandia, Szwajcaria) i ma miesięczny limit danych 10 GB. Wymaga założenia konta do korzystania z programu.

Kod DVD: 066, Licencja: Freeware, **Rejestracja:** Tak, **Język:** polski

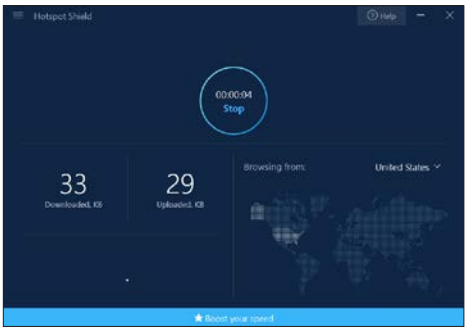
PRIVATE TUNNEL



Jest to jeden z ciekawszych programów do korzystania z sieci VPN. Wykorzystuje protokół OpenVPN i pozwala na łączenie się z siecią serwerów rozmieszczonych na całym świecie. Na bazie darmowego programu i protokołu stworzono aplikację, która zapewnia maksimum ochrony, a dzięki płatnym serwerom – jedną z najwyższych wydajności. Do dyspozycji użytkownika w wersji darmowej jest tylko 200 MB transferu miesięcznie.

Kod DVD: 046, Licencja: Freeware, **Rejestracja:** Nie, **Język:** angielski

HOTSPOT SHIELD



Jeden z najprostszych w obsłudze programów, które umożliwiają bezpieczne przeglądanie internetu poprzez wykorzystanie tunelowego połączenia w sieci VPN. Taki tunel uniemożliwia osobom trzecim podsłuchanie naszych rozmów, sprawdzanie historii przeglądania i innych aktywności wykonywanych w sieci. Nie ma funkcji automatycznego wyboru najlepszego serwera. **Uwaga!** Wymaga podania danych karty kredytowej do rozpoczęcia okresu próbnego. Jeśli nie chcemy za niego płacić, musimy pamiętać, by zrezygnować w odpowiednim terminie.

Kod DVD: 020, Licencja: Trial (karta kredytowa), **Rejestracja:** Nie, **Język:** angielski

HIDE.ME

Program do bezpiecznego surfowania w internecie. Jego główne zalety to aż 2 GB darmowego transferu każdego miesiąca. Podlega pod jurysdykcję Malezji i nie zapisuje żadnych danych dotyczących logów użytkownika. Ma również kilka wad, z których największa to dość ograniczona liczba serwerów w darmowej wersji programu, słaba pomoc techniczna i dosyć wolny transfer danych. Obsługa programu jest bardzo prosta i w skrócie sprowadza się do aktywacji okresu próbnego (który można odnawiać w nieskończoność) i połączenia się z serwerem VPN.

Kod DVD: 019, Licencja: Trial, **Rejestracja:** Nie, **Język:** polski

V

NA NASZYM DVD

TUNNELBEAR

Jeden z najlepszych programów do bezpiecznego łączenia się z internetem. Dzięki niemu możemy łączyć się anonimowo z witrynami bez ujawniania swoich danych. Serwery rozmieszczone są w różnych miejscach na całym świecie, dzięki czemu bez problemu ominiemy blokady, na przykład w serwisie YouTube, ograniczające możliwość oglądania filmów w naszym kraju. TunnelBear sprawdzi się idealnie w rękach początkujących użytkowników. Do naszej dyspozycji w ciągu miesiąca za darmo dostępny jest pakiet 500 MB transferu.

Kod DVD: 061, Licencja: Freeware, **Rejestracja:** Tak, **Język:** angielski

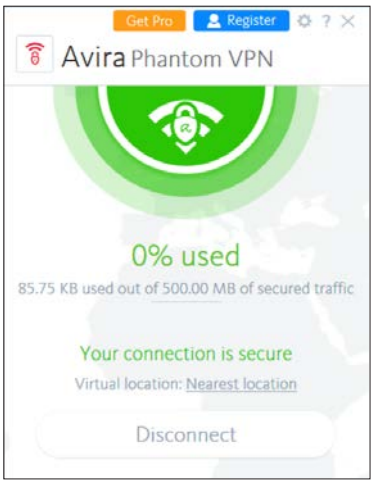
SURFEASY

W darmowej wersji programu do dyspozycji użytkownika jest 500 MB transferu do wykorzystania miesięcznie. Twórcy zapewniają, że usługa jest aktywna i sprawna przez ponad 99,9 procent czasu w skali roku, co jest niezwykle istotne, jeśli zależy nam na stabilnym bezpiecznym łączu. SurfEasy w wersji darmowej nie pozwala na korzystanie z sieci Torrent oraz nie do końca wymazuje wszystkie ślady sieciowe użytkownika. Plus to natomiast możliwość korzystania z jednego konta na aż pięciu różnych urządzeniach.

Kod DVD: 056, Licencja: Freeware, **Rejestracja:** Tak, **Język:** angielski

AVIRA PHANTOM VPN FREE

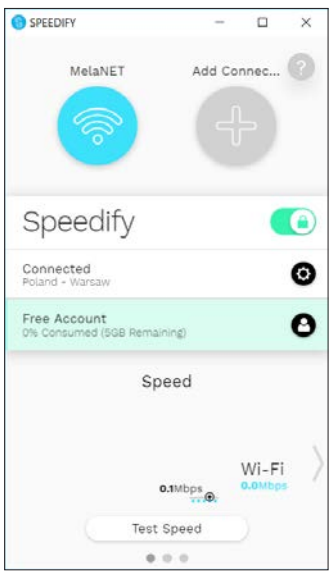
Dodatkowy pakiet firmy Avira, który umożliwia korzystanie z darmowego połączenia z zabezpieczoną siecią VPN. Miesięcznie za darmo możemy skorzystać z 500 MB transferu. Do naszej dyspozycji jest bardzo dużo serwerów, które nie są zablokowane w darmowej wersji, jak często ma to miejsce w innych programach tego typu. Niestety, jeśli zależy nam na szybkości połączenia, Avira Phantom może nie spełnić naszych oczekiwań – szybkość jest dość mierna (patrz strona 85).



Kod DVD: 005, Licencja: Freeware, **Rejestracja:** Nie, **Język:** angielski

SPEEDIFY

Speedify to bardzo nowocześnie wyglądająca aplikacja, która pozwala na korzystanie z szyfrowanego połączenia z siecią VPN. Do dyspozycji użytkownika jest wiele serwerów dostępnych w różnych lokalizacjach na całym świecie, a dodatkowo możemy wybierać pomiędzy na przykład najszybszym serwerem lub serwerem, który umożliwia korzystanie z sieci Torrent. Niestety, w naszym teście (patrz strona 85) wydajność serwerów okazała się tak słaba, że ten program nadaje się najwyżej do przeglądania witryn w internecie. **bs**



Kod DVD: 055, Licencja: Freeware, **Rejestracja:** Nie, **Język:** angielski

Więcej programów VPN oraz zestawienie prędkości pobierania znajdziemy w poradniku na stronie 84.

Fot. Anton Balazh/123rf.com

TRIKI
DO INTERNETU
KONFIGURACJA DYSKU SIECIOWEGO NAS

NASZA PRYWAT

Każdy z nas korzysta z dysków chmurowych – Dropboxa, Dysku Google, OneDrive'a. A gdyby tak stworzyć własną chmurę, by ***móc być pewnym prywatności*** *przechowywanych w niej danych? To wcale nie jest trudne!*

Do dobrych rzeczy łatwo się przyzwyczaić. Tak też jest z usługami przechowywania danych w chmurze. Jeszcze kilka lat temu Dropbox, będący pierwszym z takich serwisów, któremu udało się zdobyć popularność, krytykowany był przez sceptycznie nastawione do takich rozwiązań osoby. Dziś niemal każdy mniej lub bardziej świadomie korzysta z możliwości przechowywania danych w internecie, ale używanie najpopularniejszych rozwiązań, jak wcześniej wspomniany Dropbox, Dysk Google czy OneDrive, nie zawsze jest najlepszym sposobem na zdalny dostęp do plików, choć z pewnością ma swoje zalety.

Czym jest chmura i jak działa?

Ogólnodostępne i w podstawowych wariantach darmowe usługi przechowywania danych w chmurze na początku pozwalały jedynie przesłać pliki do internetu i mieć do nich dostęp z różnych urządzeń. Dziś są w stanie analizować nasze dane i w różny sposób je edytować, oferując dodatkowe funkcje. Działanie takiej chmury w podstawowych jej aspektach jest proste. Usługodawca udostępnia określoną ilość miejsca na swoich serwerach klientom, którzy za pośrednictwem internetu mogą przesyłać tam dane i mieć do nich dostęp z każdego miejsca na świecie oraz z dowolnego urządzenia, oczywiście po potwierdzeniu tożsamości.

Chmura to nie tylko przechowywanie danych, to także ich obróbka

Dzisiejsze usługi chmurowe to nie tylko magazynowanie danych. Najlepszym przykładem na ich ogromny potencjał są Zdjęcia Google. Ta usługa służy do przechowywania, poddawania prostej edycji i udostępniania plików graficznych. Z roku na rok oferuje coraz więcej funkcji, z których większość wspomagana jest sztuczną inteligencją. Przegląda ona nasze zdjęcia i analizuje je, żeby ułatwić ich wyszukiwanie. Dzięki maszynowemu uczeniu jest ona w stanie rozpoznać różne elementy na fotografiach i kategoryzować je. Dlatego, gdy wpiszemy w wyszukiwarce Zdjęć Google na przykład słowo plaża, w wynikach wyświetlone zostaną wszystkie zdjęcia, na których widać plażę, nawet jeśli w nazwie plików nie ma tego słowa. Ten sam trik możemy wykorzystać w odniesieniu do najróżniejszych krajobrazów, przedmiotów, zwierząt, a nawet ludzi. W Polsce funkcja rozpoznawania twarzy nie jest dostępna, ale użytkownicy w innych krajach mogą wpisać imię, żeby w wynikach wyszukiwania odnaleźć fotografie, na których jest wskazana osoba. Zdjęcia Google po analizie plików graficznych proponują także poprawienie niektórych parametrów, jak jasność czy nasycenie barw, mogą tworzyć animacje, albumy, a także kolaże. Za tym wszystkim stoi sztuczna inteligencja oraz maszynowe uczenie.
Jednak ogólnodostępne usługi chmurowe mają też swoje wady.

Bezpieczeństwo danych i prywatność w chmurze

Dane przechowywane w znanych usługach chmurowych są względnie bezpieczne, bo każda z firm mających w swojej ofercie dyski online dba o to, żeby pliki klientów nie trafiły w niepowołane ręce. Jednak najpopularniejsze usługi przechowywania danych w internecie są łakomym kąskiem dla hakerów. Najlepszym przykładem na to, że nawet największe firmy mogą paść ich ofiarą, jest znana afera dotycząca wykradzionych z usługi iCloud od Apple i opublikowanych w internecie prywatnych zdjęć aktorek oraz modelek. To jednostkowy przypadek, ale nikt nie jest w stanie zagwarantować, że takie sytuacje nie powtórzą się w przyszłości.
To, a także fakt, że do naszych danych mają dostęp usługodawcy, może rodzić obawy dotyczące

NA CHMURA

naszej prywatności. Jeśli szukamy usługi chmurowej, w której do przechowywanych danych będziemy mieć dostęp tylko my i wskazane osoby, możemy zainwestować w sieciowy serwer plików NAS. Dzięki takiemu rozwiązaniu będziemy mogli nie tylko stworzyć własną i prywatną chmurę na dane, ale także korzystać z wielu funkcji, które oferują takie urządzenia.

NAS, czyli sieciowy serwer plików

NAS-y to stosunkowo małe urządzenia służące jako sieciowe serwery plików. Dzięki nim w prosty sposób możemy w domu współdzielić dane pomiędzy różnymi urządzeniami.

Nie muszą to być tylko komputery. Do plików mogą mieć dostęp wszystkie urządzenia podpięte do sieci domowej, także smartfony oraz telewizory.

NAS-y mają więcej zalet, ale zależą one od urządzenia, które wybierzemy.

W polskich sklepach znajdziemy proste w obsłudze serwery sieciowe gotowe do pracy zaraz po wyjęciu z pudełka. Wymagają one tylko podstawowej konfiguracji i po kilku minutach można z nich korzystać. Kolejną zaletą jest to, że producent wyposażył je w dyski twarde, więc nie musimy kupować ich osobno. Do takich urządzeń należą **Seagate Personal Cloud**, **Western Digital My Cloud**, **Western Digital My Cloud Home**.

Inną kategorią są bardziej zaawansowane NAS-y, oferujące dużo większe możliwości. Takie urządzenia mogą stać się nie tylko serwerami plików, ale także miejscem do przechowywania i zautomatyzowania kopii zapasowych danych z różnych urządzeń, a nawet domowym centrum rozrywki. Najtańszymi urządzeniami z tej kategorii są jednozatokowe NAS-y, do których niestety trzeba dokupić dysk twardy we własnym zakresie. W ich wypadku trzeba też poświęcić trochę więcej czasu na konfigurację sprzętu, żeby w pełni wykorzystać wszystkie jego możliwości. Do takich NAS-ów zaliczają się **Synology DS115j** czy **QNAP TS-128A**.

Ostatnia kategoria to NAS-y wielozatokowe, z których największą popularnością wśród użytkowników domowych cieszą się modele mieszczące dwa dyski twarde. Oprócz wszystkich zalet wcześniej wspomnianych urządzeń mają także inne zalety, z których najważniejszą jest możliwość stworzenia macierzy RAID 1 zwiększającej bezpieczeństwo danych. W tak skonfigurowanym NAS-ie każdy plik przechowywany jest jednocześnie na dwóch dyskach, więc w razie awarii jednego z nich pliki można odtworzyć bez najmniejszych problemów z drugiego. NAS-y wielozatokowe często wyposażane są przez producentów w więcej pamięci RAM, wydajniejsze procesory, a nawet piloty pozwalające sterować urządzeniem z kanapy. Wiąże się to oczywiście z wyższą ceną, ale decydując się na takie urządzenie, dostajemy najwięcej możliwości, a NAS podłączony do telewizora może pełnić nawet

funkcję komputera. Do takich modeli zaliczyć możemy **Synology DS216j**, **Synology DS218+**, **QNAP TS-253B-8G**, **QNAP TS-251A**, **Asustor AS3202T**.

NAS – zalety i wady

Największą zaletą wykorzystania NAS-ów jako prywatnej chmury jest dużo wyższy poziom bezpieczeństwa, o ile tylko odpowiednio skonfigurujemy urządzenie. W takim przypadku dostęp do danych będziemy mieć tylko my i osoby, którym je udostępnimy. To zdecydowanie najbezpieczniejszy sposób na przechowywanie danych. Kolejna zaleta prywatnej chmury to miejsce na dane ograniczone wyłącznie pojemnością dysków twardych zainstalowanych w serwerze. Podobnie jak w przypadku chmury publicznej, tak też w prywatnej możemy mieć dostęp do plików z niemal każdego miejsca na świecie, potrzebne będzie wyłącznie połączenie z internetem.

Systemy operacyjne zainstalowane na NAS-ach zostały wyposażone w narzędzia ułatwiające synchronizację danych między serwerem i komputerami oraz smartfonami, nie musimy więc martwić się ręcznym przerzucaniem plików.

W porównaniu ze znanymi usługami chmurowymi NAS-y mają też wady. Pierwszą i być może najważniejszą jest cena urządzeń. Za modele oferujące najwięcej możliwości trzeba zapłacić 1000 złotych i więcej, a do tego należy doliczyć cenę dysków twardych. W zależności od ich pojemności cena za kompletny sieciowy serwer plików może sięgnąć lub nawet przekroczyć 2000 złotych. Prywatność, niestety, kosztuje.

Kolejną wadą takiego rozwiązania jest brak sztucznej inteligencji obecnej chociażby w opisywanej wcześniej usłudze Zdjęcia Google. Nie będziemy mogli liczyć na to, że aplikacja zaproponuje automatyczną zmianę parametrów zdjęć, przeszuka pliki graficzne według ich zawartości, a albumy, kolaże i animacje będziemy musieli tworzyć sami.

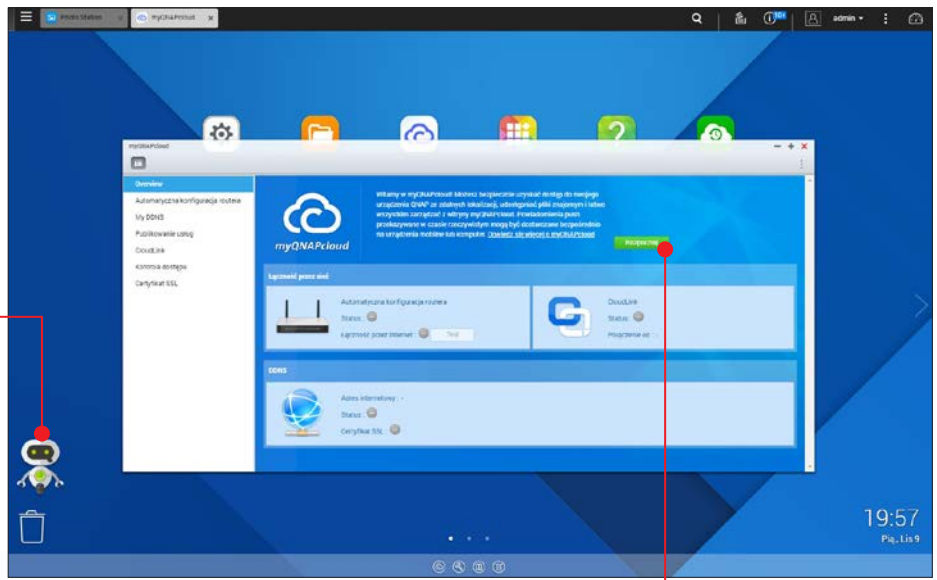
Odpowiednio skonfigurowany NAS to nie tylko prywatna chmura. To także wiele innych funkcji polegających głównie na przechowywaniu plików. Sieciowy serwer plików ułatwia i automatyzuje tworzenie kopii bezpieczeństwa plików, a nawet obrazów całych partycji, a także dysków. NAS bardzo łatwo przekształcić także w domowe centrum rozrywki udostępniające pliki multimedialne wszystkim urządzeniom w domu.

Doinstalowanie aplikacji **Plex** (do pobrania z KŚ+ – www.ksplus.pl) pozwala bardzo wygodnie przeglądać i odtwarzać filmy. Program nawet w darmowej wersji pobiera z internetu takie dane dotyczące plików wideo, jak plakaty, opisy, oceny z serwisu IMDB, i w atrakcyjny sposób prezentuje je na ekranach telewizorów i komputerów.

NAS to dużo więcej zastosowań. Zwłaszcza modele droższe od QNAP i Synology pozwalają na dodawanie nowych funkcji do urządzeń przez pobieranie programów z oficjalnych lub nieoficjalnych repozytoriów, dzięki czemu sieciowy serwer plików może nawet zarządzać inteligentnymi urządzeniami w naszych domach. **tk**

KONFIGURACJA SERWERA NAS DO PRACY W ROLI PRYWATNEJ CHMURY

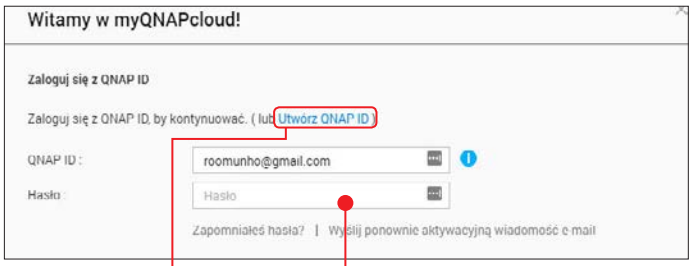
Konfigurację serwera NAS pokażemy na przykładzie systemu operacyjnego **QTS** dostępnego na urządzeniach firmy **Qnap**.



1 Pierwszym krokiem w celu skonfigurowaniu NAS-a do pracy jako prywatnej chmury jest włączenie usługi **myQNAPcloud** i zarejestrowanie się w niej. Pomaga w tym kreator, do którego skrót znajduje się na pulpicie.

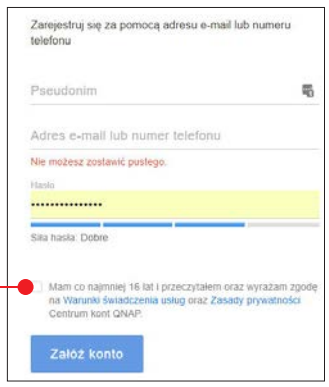
2 Po uruchomieniu aplikacji należy kliknąć na przycisk **Rozpocznij** w górnej części okna i postępować zgodnie ze wskazówkami.

3 Kolejnym krokiem jest zalogowanie się w usłudze myQNAPcloud. Jeśli korzystamy z niej po raz pierwszy, konieczne będzie zało-



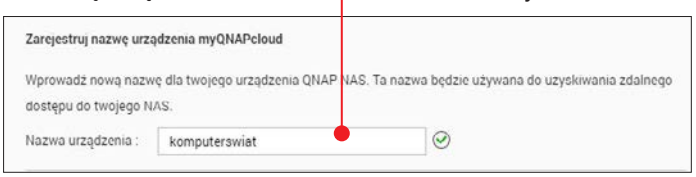
żenie konta oraz zarejestrowanie urządzenia. W tym celu należy kliknąć na **Utwórz QNAP ID**.

4 Zostaniemy przeniesieni do strony internetowej pozwalającej założyć konto w usłudze. Po uzupełnieniu pól **Pseudonim**, **Adres e-mail** i **hasło** oraz zaznaczeniu pola potwierdzającego, że mamy więcej niż 16 lat, nasze konto zostanie założone.



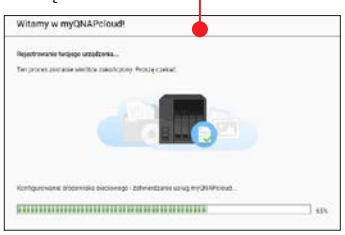
5 Kiedy będziemy mieli dane logowania, możemy wrócić do pulpitu systemu QTS i zalogować się w usłudze.

6 W kolejnym oknie wybieramy nazwę urządzenia.



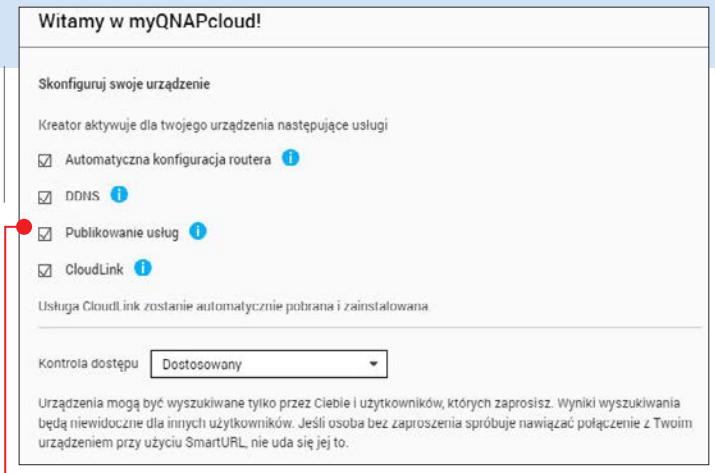
7 W następnym oknie zaznaczamy wszystkie pola wyboru oraz ustawiamy poziom kontroli dostępu. **Publiczny** oznacza, że nasze urządzenie i udostępniane przez nie usługi będą mogły być wyszukiwane przez innych użytkowników myQNAPcloud. **Prywatny** daje dostęp do urządzenia tylko nam, a **Dostosowany** pozwala wskazać dodatkowe osoby, które mogą łączyć się z NAS-em.

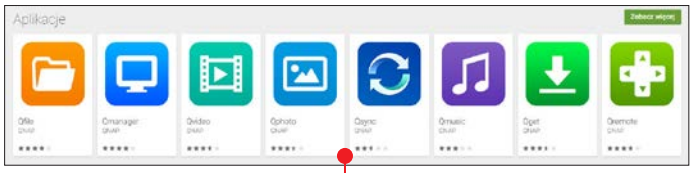
8 Kolejny etap to automatyczna konfiguracja i rejestracja urządzenia.



9 Ostatnie wyświetlane okno przedstawia podsumowanie informacji dotyczących uruchomionej usługi myQNAPcloud.

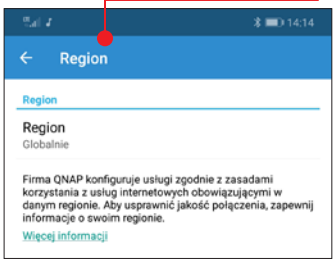
10 Tak skonfigurowany NAS daje już dostęp do plików z internetu. Żeby móc z nich korzystać na komputerach, należy zalogować się w przeglądarce w usłudze myQNAPcloud (**www.myqnapcloud.com**).





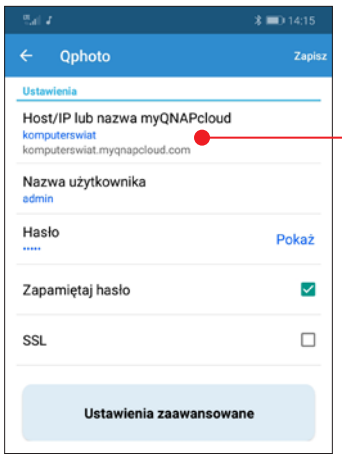
11 Tym, co jeszcze należy zrobić, jest zainstalowanie i konfiguracja aplikacji mobilnych, dających wygodny dostęp do plików przechowywanych na NAS-ie. Ze sklepu Goo gle Play lub App Store należy pobrać programy według uznania: **Qfile** (menadżer plików), **Qvideo** (zarządzanie filmami), **Qmusic** (strumieniowanie muzyki), **Qphoto** (dostęp do zdjęć) i **Qsync** (automatyczna synchronizacja danych między urządzeniem mobilnym i serwerem NAS).

12 Ich konfiguracja jest prosta i w każdym przypadku wygląda tak samo. Po uruchomieniu aplikacji w pierwszym oknie nie zmieniamy nic, pozostawiając domyślne ustawienia regionu.



13 Następnie konieczne będzie dodanie serwera NAS za pomocą przycisku **Dodaj NAS ręcznie** w dolnej części ekranu.

14 W kolejnym kroku uzupełniamy pola **Host/IP lub nazwa myQNAPcloud** (podana w czasie konfigurowania usługi), nazwa użytkownika oraz hasło, po czym zatwierdzamy wprowadzone dane przyciskiem **Zapisz** (górny prawy róg ekranu).



15 Po połączeniu z NAS-em zostaną w aplikacji wyświetlone nasze pliki.

Fot. Felix Pergande, Denchik/123rf.com

TRIKI DO INTERNETU
DWUETAPOWA WERYFIKACJA KONTA

PODWÓJNIE PEW

*Korzystanie z poczty elektronicznej to codzienność. Większość z nas swoje skrzynki e-mailowe założyła lata temu i korzysta z nich regularnie, jednak nie dba o ich **bezpieczeństwo**. A to oznacza zagrożenie prywatności. Przeczytajmy, jak temu zaradzić*

Niezabezpieczona skrzynka odbiorcza to łakomy kąsek dla hakerów. Kiedy myślimy o włamaniu na nasze konto poczty elektronicznej, w pierwszej chwili martwimy się o przechowywaną w internecie korespondencję nie tylko prywatną, ale także prowadzoną z różnymi instytucjami, również finansowymi. Zagrożeń jest jednak więcej.

Jeśli ktoś niepowołany uzyska dostęp do naszej skrzynki odbiorczej, nie tylko pozna czasem bardzo wrażliwe dane dotyczące naszego życia, ale będzie mógł także w bardzo łatwy sposób przejąć kontrolę nad naszymi kontami w innych usługach, jak na przykład serwisy społecznościowe i – co gorsza – usługi bankowości internetowej. Wszystko to dzięki możliwości szybkiego zresetowania hasła w serwisach skojarzonych z adresem e-mail. Dlatego tak ważne jest odpowiednie zabezpieczenie poczty elektronicznej.

Podstawowa zasada, którą powinniśmy wcielić w życie, to częsta zmiana hasła oraz stosowanie w nim losowych znaków składających się z małych i dużych liter, cyfr, a także znaków specjalnych.

Wielu dostawców usług poczty elektronicznej wprowadziło dodatkowe zabezpieczenie, jakim jest weryfika-

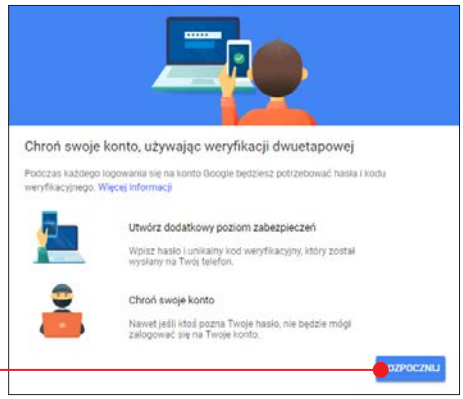
JAK PODWÓJNIE ZABEZPIECZYĆ GMAILA

Z włączaniem dwuetapowej weryfikacji zapoznamy się na przykładzie najpopularniejszej usługi poczty elektronicznej – Gmail. Jej twórca, firma Google, pozwala użytkownikom zabezpieczyć skrzynki odbiorcze na wiele sposobów, więc będzie to przy okazji dobry przykład na pokazanie różnych form weryfikacji dwuetapowej.

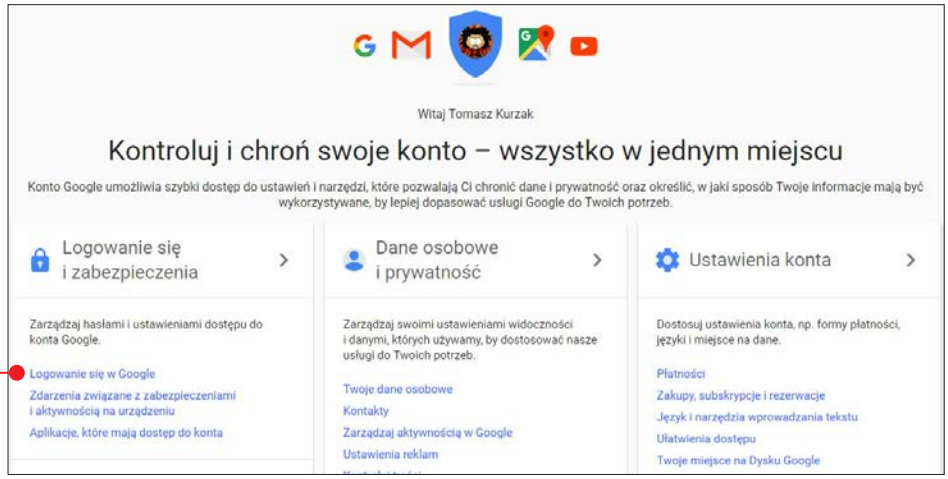
1 Żeby uzyskać dostęp do ustawień bezpieczeństwa poczty Gmail, należy zalogować się na swoim koncie Google pod adresem **https://myaccount.google.com/intro?hl=pl**

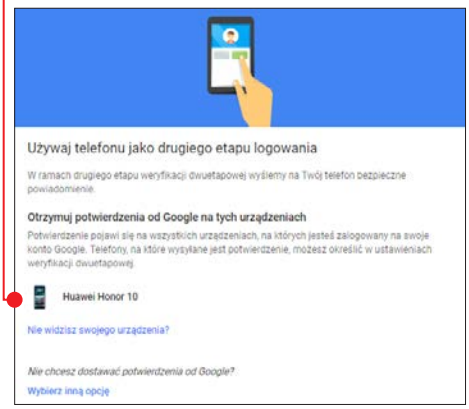
2 Następnie w sekcji **Logowanie się i zabezpieczenia** klikamy na **Logowanie się w Google** i w nowym oknie przechodzimy do ustawień związanych z weryfikacją dwuetapową.

3 Kolejny ekran informuje o tym, że włączenie dwuetapowej weryfikacji będzie wiązało się z koniecznością podawania dodatkowego kodu w czasie logowania się w usługach Google. Na tym etapie klikamy na przycisk **Rozpocznij**, żeby zainicjować procedurę.



4 Pierwszą z zaproponowanych metod uwierzytelniania jest usługa, która przy każdej próbie logowania do konta Google wyświetla na skojarzonym z nim smartfonie z Androidem komunikat z prośbą o autoryzację. Jest to bardzo wygodny sposób, który ma jeszcze jedną zaletę: kiedy tylko ktoś będzie próbował zalogować się na nasze konto, zostaniemy o tym powiadomieni.





NE KONTA

cja dwuetapowa. Polega ona na tym, że poza wpisaniem tradycyjnego loginu i hasła użytkownicy muszą potwierdzić swoją tożsamość za pomocą specjalnego kodu wysyłanego na wskazane wcześniej urządzenie. W większości przypadków kody są generowane automatycznie i mają ograniczony czas ważności. Dzięki temu tylko prawdziwy właściciel może uzyskać dostęp do poczty.

Sposoby wysyłania kodu

Sposobów na przesłanie kodu do użytkownika jest kilka. Najpopularniejszym jest SMS przesyłany na wcześniej podany numer telefonu i zawierający odpowiedni ciąg znaków.

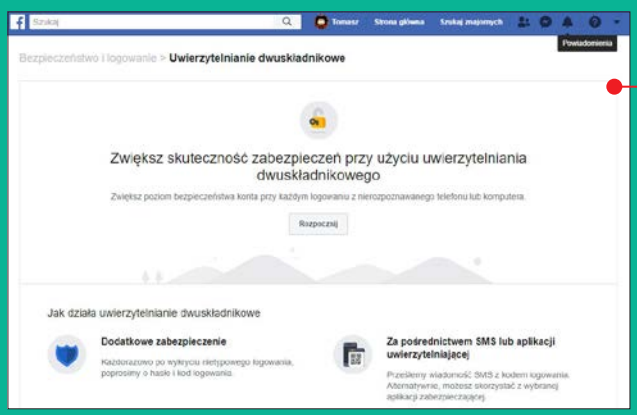
Możliwe jest także wykonanie przez dostawcę usługi połączenia telefonicznego, w którym automat dyktuje znaki, które należy wpisać podczas logowania.

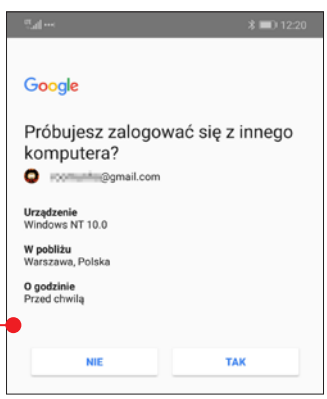
Są także specjalne aplikacje mobilne, które po odpowiedniej konfiguracji generują automatycznie kody zabezpieczające i zmieniają je w ustalonych odstępach czasu.

tk

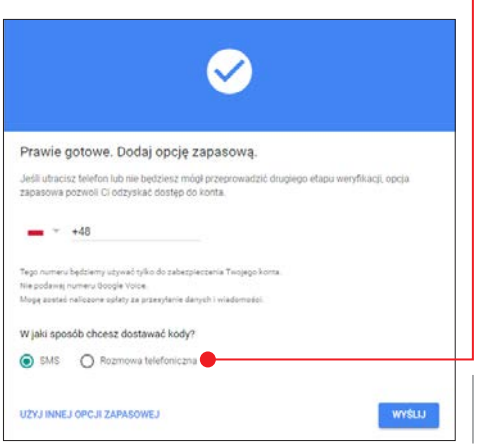
ZABEZPIECZ NIE TYLKO POCZTĘ

Za pomocą weryfikacji dwuskładnikowej powinniśmy zabezpieczyć nie tylko pocztę elektroniczną. Także takie usługi jak Facebook, Steam, Origin, a w szczególności serwisy bankowości internetowej należy zabezpieczać dodatkowo, żeby chronić nie tylko informacje o nas, ale przede wszystkim pieniądze.



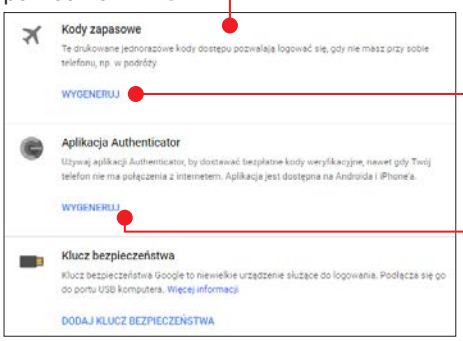


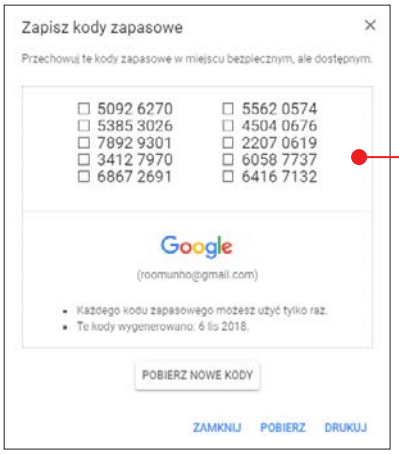
5 Jeśli zdecydujemy się na ten sposób weryfikacji, będziemy musieli ustawić jeszcze jeden, który pozwoli nam zalogować się, jeśli nie będziemy mogli skorzystać z wcześniej opisanej metody. Pierwszą proponowaną przez Google jest przesłanie SMS-a lub połączenie głosowe na podany przez użytkownika numer telefonu komórkowego.



Efektem tych działań będzie włączenie dwuetapowej weryfikacji potwierdzane za pomocą każdego urządzenia, na którym jesteśmy zalogowani.

6 Konto Google pozwala także zweryfikować tożsamość użytkownika na trzy inne sposoby: za pomocą listy kodów zapasowych, przy użyciu przeznaczonej na urządzenia mobilne aplikacji **Authenticator** lub z wykorzystaniem specjalnego klucza USB. Każdą z tych opcji możemy skonfigurować, klikając na odpowiednie linki.





7 Warto rozważyć dodanie kolejnej opcji uwierzytelniania na wypadek, gdybyśmy stracili dostęp do smartfona, na który będą wysyłane komunikaty z potwierdzeniem tożsamości lub SMS-y z kodem. Najlepiej w takich sytuacjach sprawdzą się kody zapasowe, które można wydrukować i przechowywać w bezpiecznym miejscu. Żeby mieć do nich dostęp, wystarczy kliknąć na **Wygeneruj** w polu **Kody zapasowe**.

8 Poręczną formą uwierzytelniania są także aplikacje generujące kody na bieżąco jak **Google Authenticator** lub **Authenticator** od Last Pass. Żeby z nich skorzystać, wystarczy kliknąć na **Wygeneruj** w polu **Aplikacja Authenticator** wybrać wersję systemu zainstalowaną na smartfonie (Android lub iOS), a następnie zeskanować wygenerowany kod QR wybranym przez nas programem.

Fot. Eugene Sergeev/123rf.com

TRIKI DO INTERNETU
SKRZYNKI E-MAIL TYMCZASOWE I Z SZYFREM

S NE SKRZ TYMCZASOWE I

*Poznajmy **skrzynki pocztowe do zadań specjalnych**: tymczasowe, do których możemy na przykład kierować niechciane wiadomości, oraz szyfrowaną, która zapewni nam prywatność*

W internecie znajdziemy bardzo wiele serwisów oferujących możliwość zakładania szybkich kont e-mailowych, które będziemy mogli wykorzystać na przykład, gdy jakaś usługa czy aplikacja, której nie ufamy, będzie chciała poznać nasz adres e-mail. W dużej ilości przypadków podawanie naszego adresu mniej znanym i zaufanym aplikacjom kończy się tym, że nasza skrzynka pocztowa jest zasypywana niechcianymi wiadomościami. Dzięki możliwości korzystania z tymczasowych adresów e-mail będziemy w stanie uwolnić się od fali spamu. Serwisy świadczące takie usługi różnią się od siebie, ale zasada ich działania jest taka sama. Nie zapewniają one użytkownikom ochrony danych, gdyż nie wymagają rejestracji i podawania hasła. Uważajmy również, do jakich usług przypisujemy jednorazowe konta e-mail. Jeśli jest to dla nas ważne konto na przykład ze sklepu internetowego, w którym robimy często zakupy, lepiej podać nasz prawdziwy adres e-mail.

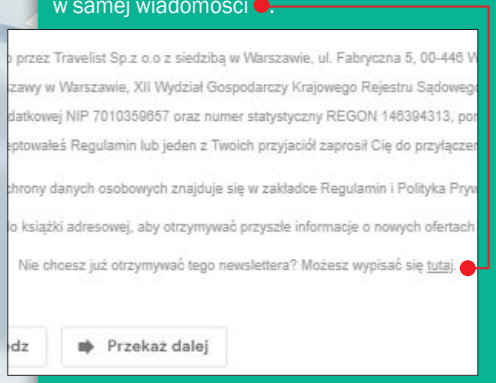
Inną kategorią ciekawych skrzynek e-mail są skrzynki szyfrowane wiadomości i w ten sposób dbające o naszą prywatność. Przedstawiona na stronie obok poczta Tutanota automatycznie szyfruje całą komunikację e-mail. Nie musimy wykonywać żadnych skomplikowanych instrukcji – nasza poczta wszystko to robi za nas. **kd**

SPAM

To niepożądane i niechciane wiadomości elektroniczne. Aby wiadomość mogła być uznana za spam, musi spełniać trzy podstawowe warunki:

- Treść otrzymanej wiadomości jest całkowicie niezależna od naszej tożsamości.
- Nie wyraziliśmy wcześniej zgody na otrzymywanie takiej wiadomości.
- Sama treść wiadomości sugeruje, że nadawca poprzez rozpowszechnianie takiej wiadomości może odnieść zyski nieproporcjonalne do korzyści odbiorcy.

Wszystkie wiadomości otrzymywane po zapisaniu się do newsletterów, nawet jeśli przychodzą do nas bardzo często, nie zaliczają się do tak określonej kategorii spamu, ponieważ sami wyraziliśmy zgodę na ich otrzymywanie. Najczęściej możemy z nich zrezygnować, klikając na odpowiedni odnośnik w samej wiadomości.



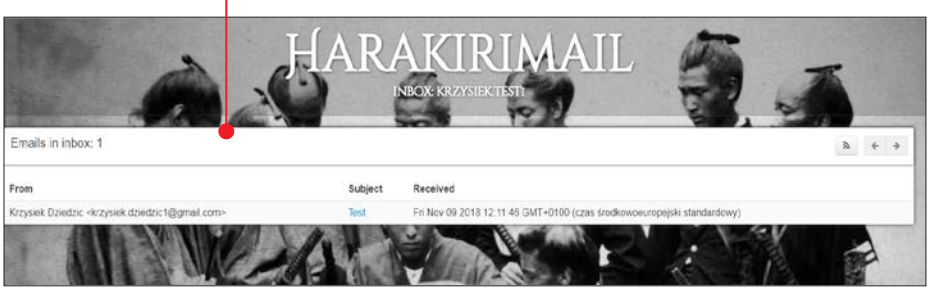
HARAKIRIMAIL

Tę tymczasową skrzynkę możemy przeznaczyć na przykład na wiadomości reklamowe ze sklepów internetowych i innych usług. Wiadomości przechowywane są w niej przez 24 godziny, a następnie kasowane.

Aby utworzyć konto, na głównej stronie tego serwisu klikamy na losowo wygenerowany adres e-mail widoczny w polu. Nie musimy nawet sami wymyślać nazwy dla naszego konta.

W głównym interfejsie skrzynki nie znajdziemy zbyt wielu funkcji. Nie możemy usuwać wiadomości ani na nie odpowiadać. Harakirimail oferuje tylko i wyłącznie usługę odbierania wiadomości na wybraną skrzynkę przez 24 godziny – później musimy wygenerować kolejną skrzynkę.

Skrzynkę znajdziemy na stronie **www.harakirimail.com**



YNKI E-
Z SZYFREM

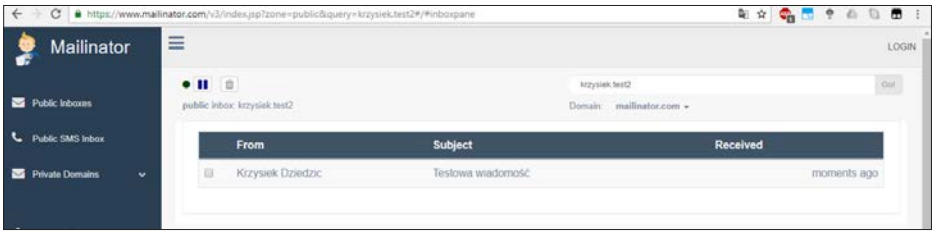
TESTOWANIE USŁUG POD KĄTEM SPAMU

Dobrym pomysłem jest wykorzystanie tymczasowej skrzynki do sprawdzania nowych aplikacji czy usług. Jeśli okaże się, że wysyłają one do nas dużo wiadomości, pozostawmy je w skrzynce tymczasowej. Jeżeli jednak nie będą wysyłać zbędnych informacji, możemy rozważyć zmianę adresu usługi na ten, z którego korzystamy na co dzień.

MAILINATOR

Serwis umożliwiający założenie tymczasowej skrzynki e-mail, którą możemy wykorzystywać do rejestracji w witrynach, którym nie ufamy lub które podejrzewamy o rozsyłanie uciążliwych wiadomości. E-maile otrzymywane na tymczasową skrzynkę są usuwane po kilku godzinach.

Nie należy korzystać z tej usługi do potwierdzenia rejestracji ważnego dla nas konta lub takiego, które zawiera jakieś prywatne dane, gdyż skrzynka nie jest zabezpieczona hasłem, a wiadomości nie są szyfrowane. Dodatkowo warto wiedzieć, że ta poczta nie pozwala na odczytywanie załączników, umożliwia odczytywanie tylko i wyłącznie samej treści wiadomości przychodzących.



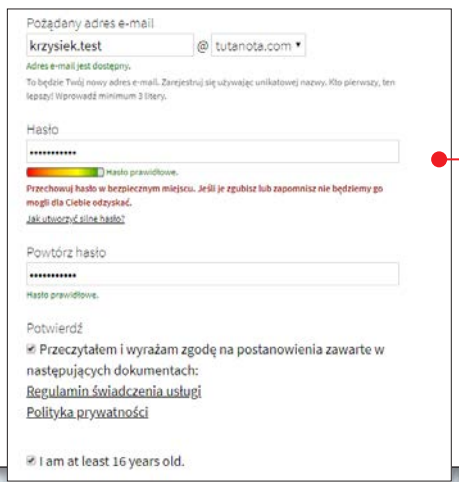
Interfejs Mailinatora jest nieco bardziej rozbudowany niż Harakirimail; po wykupieniu płatnej wersji możemy uzyskać dostęp do dodatkowych funkcji, na przykład zmiany domeny z **mailinator.com** na inną dostępną wybraną przez nas. Skrzynkę znajdziemy pod adresem **www.mailinator.com**

TUTANOTA

Tutanota to nieco innego rodzaju skrzynka pocztowa – nie jest ona tymczasowa, jak poprzednie usługi. Musimy przejść przez proces rejestracji i założyć konto. Uzyskamy wtedy dostęp do skrzynki pocztowej, która szyfruje wszystkie wiadomości i dba o naszą prywatność. Nawet temat i załączniki są bezpiecznie szyfrowane. Ze skrzynki Tutanota możemy bezpiecznie korzystać w dowolnej przeglądarce, a nawet na urządzeniach mobilnych dzięki specjalnej aplikacji. Skrzynka jest całkowicie darmowa i po założeniu konta do dyspozycji użytkownika jest 1 GB miejsca na dane.

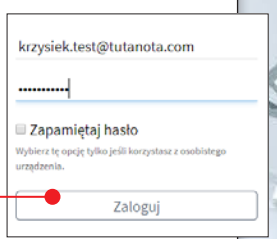
Zakładamy konto

1 Po wejściu na stronę **tutanota.com** klikamy na **Zarejestruj się** na środku ekranu.



2 Następnie uzupełniamy formularz. W pierwszym wierszu wybieramy domenę naszej skrzynki i po zatwierdzeniu zgód klikamy na **Utwórz konto**.

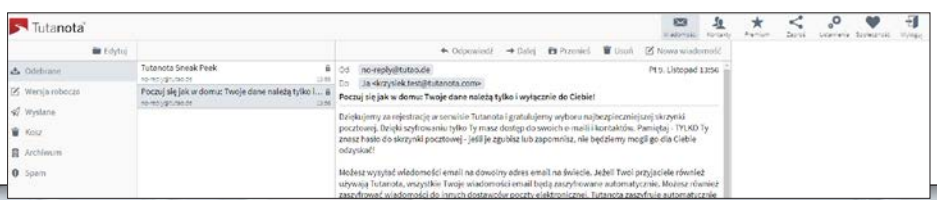
3 Po utworzeniu konta możemy zalogować się, korzystając z podanych wcześniej danych i klikając na **Zaloguj**.



Interfejs skrzynki jest minimalistyczny i przejrzysty. Wszystkie funkcje są łatwo dostępne, a obsługa nie powinna stanowić problemu nawet początkującym.

Szyfrowanie wiadomości

Uwaga! Tutanota pozwala na automatyczne wysyłanie zaszyfrowanych wiadomości tylko i wyłącznie pomiędzy użytkownikami, którzy korzystają z usług Tutanota. Jeśli jedna z osób ma skrzynkę w innym serwisie, wiadomości nadal będą bez problemów dochodzić, lecz nie będą szyfrowane.



Fot. Sergey Nivens/123rf.com

9 PROSTYCH SPOSOBÓW *NA ZAPEWNIENIE SOBIE PRYWATNOŚCI W INTERNECIE*

Żyjemy w czasach, kiedy informacja jest na wagę złota. O prywatność w sieci warto i trzeba dbać. Komputer Świat często pisze o sposobach na zachowanie prywatności i anonimowości. A oto dziewięć prostych zasad (które można znaleźć na stronie internetowej New York Timesa) stanowiących dobre podsumowanie tego, co można przeczytać w tym wydaniu Komputer Świat Special. **pk**

1 Korzystaj z komunikatorów szyfrujących

Szyfrowanie jest skutecznym sposobem na ochronę wrażliwych danych. Warto z niego korzystać nie tylko do zabezpieczania danych, ale też podczas prywatnych rozmów tekstowych. Wystarczy użyć szyfrującego wiadomości komunikatora, takiego jak **Signal** (patrz też książka z serii Biblioteczka Komputer Świata – Anonimowość w internecie).

2 Zachowaj ostrożność, klikając na linki i otwierając dokumenty

To niby oczywiste, ale ataki na naszą prywatność często są dokonywane za pomocą złośliwych załączników i linków w e-mailach. Przed phishingiem najskuteczniej chroni rozsądek – nie należy klikać na niepewne odnośniki. Trzeba też regularnie aktualizować oprogramowanie – niezaktualizowane programy mogą zawierać luki bezpieczeństwa. Warto także zainteresować się pakietami antywirusowymi, jak **Bitdefender** (na rok z prenumeratą Komputer Świata) i **ESET Internet Security** (na rok z Niezbędnikiem).

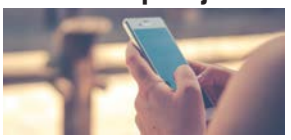
3 Zabezpiecz dysk swojego komputera

Dysk komputera jest prawdziwą kopalnią naszych danych osobowych. Aby je chronić, warto skorzystać z szyfrowania. Użytkownicy systemów Windows w wersjach 7 Ultimate oraz 8, 8.1 i 10 Professional mogą skorzystać z funkcji **Bitlocker** (patrz strona 49). A we wszystkich wersjach Windows możemy korzystać z narzędzia **VeraCrypt** (DVD-KOD: **063**) (patrz strona 46). Jeśli chcemy zabezpieczyć pliki w chmurze – skorzystajmy z **Cryptomatora** (DVD-KOD: **011/012**) (strona 48).

4 Mądrze korzystaj z haseł

Jedną z najprostszych rzeczy, które można zrobić, by chronić swoje dane w sieci, jest korzystanie z silnych haseł i mądre ich wykorzystanie. Do każdej z witryn należy mieć osobne hasło. Aby nie pogubić się wśród tylu haseł, warto korzystać z menedżerów, takich jak **Last Pass** (DVD-KOD: **032**) czy **KeePass** (DVD-KOD: **024**) i inne (patrz strona 56).

5 Korzystaj z weryfikacji dwuetapowej



Gdy to możliwe, warto włączyć drugą warstwę ochrony prywatności w postaci kodu wysyłanego na telefon. Dzięki temu ktoś, kto będzie próbować dostać się do naszych danych, natknie się na przeszkodę nie do przejścia – telefon, który zawsze mamy przy sobie. Tej metody powinno się używać w przypadku poczty, kont społecznościowych czy służbowych (patrz strona 94).

6 Korzystaj z HTTPS

Warto upewniać się, czy witryny, z których korzystamy, używają bezpiecznego protokołu **https**. Aby nie musieć robić tego za każdym razem, warto do przeglądarki dodać wtyczkę **HTTPS Everywhere** (patrz strona 63), która wymusza połączenie typu HTTPS. Dodatek ten dostępny jest dla przeglądarek Chrome, Firefox, Opera i dla Firefoxa dla Androida.

7 Korzystaj z VPN

Do ochrony danych wysyłanych za pomocą komputera i telefonu warto korzystać z VPN, czyli Virtual Private Network. Rozwiązanie to tworzy tunel, przez który można bezpiecznie przesyłać dane, jednocześnie ukrywając swoją lokalizację. Zabezpieczenie to przydaje się szczególnie, jeśli korzystamy z publicznych sieci Wi-Fi (o VPN-ach więcej od strony 84).

8 Pamiętaj, że tryb incognito nie jest całkiem prywatny

Korzystając ze zwykłej przeglądarki, warto pamiętać, że nie jesteśmy niewidzialni, nawet w trybie incognito, który nie jest w stanie ukryć naszej aktywności przed pracodawcą (jeśli korzystamy z sieci firmowej) ani przed dostawcą internetu. Nie chroni prywatności, a jedynie nie pokazuje lokalizacji i nie zapisuje historii przeglądarki. Dlatego warto znać **bezpieczne przeglądarki** (strona 44).

9 Korzystaj z bezpiecznych wyszukiwarek

Google zdominowało rynek wyszukiwania. Możemy jednak skorzystać z alternatywy w postaci **DuckDuckGo**, która zapewnia anonimowość (więcej w książce Anonimowość w internecie). Trzeba tylko pamiętać, że wyniki wyszukiwania w Google, właśnie dzięki danym, jakie są o nas zbierane, są bardziej precyzyjne.

Komputer Świat SPECIAL

Adres redakcji: 02-672 Warszawa, ul. Domaniewska 52
internet: www.komputerswiat.pl, forum.komputerswiat.pl
e-mail: redakcja@komputerswiat.pl

Rafał Kamiński (rk)
redaktor naczelny, szef wydania online

Agnieszka Al-Jawahiri (aa)
redaktor prowadzący

Mariusz Michalski (mm)
DVD manager

Paweł Krzyżanowski (pk)
autor

Dawid Długosz (dd)
autor

Krzysztof Dziedzic (kd)
autor

Konrad Jagaciak (kj)
autor

Adam Kopeć (ak)
autor

Tomasz Kurzak (tk)
autor

Agnieszka Serafinowicz (as)
autor

Bartłomiej Sieja (bs)
autor

Karol Żebruń (kż)
autor

Jolanta Rososińska
korekta

Robert Dobrzyński
dyrektor artystyczny

Mariusz Rybak
redaktor graficzny

ringier axel springer

Wydawca: RINGIER AXEL SPRINGER POLSKA Sp. z o.o.
Członek Izby Wydawców Prasy i Związku Kontroli Dystrybucji Prasy
www.ringieraxelspringer.pl, asp@axelspringer.pl
Adres: 02-672 Warszawa, ul. Domaniewska 52
tel. 22 2320000, 22 2320001

Prezes Zarządu: Mark Dekan
Prezes Honorowy: Wiesław Podkański
Dyrektor Generalny: Marcin Biegluk
Dyrektor Wydawniczy: Paweł Paczuski
Dyrektor Finansowy: Krzysztof Stopa
Dyrektor Sprzedaży: Mariusz Wąsiński
Dyrektor Marketingu: Joanna Kloskowska

media impact

Biuro reklamy: Media Impact
reklama.warszawa@mediaimpact.pl
tel. (12) 2600200 (BOK)

Business Project Manager: Paweł Bulwan
Dział personalny: Monika Remiszewska
Księgowość: Katarzyna Fita (dyrektor)
Kolportaż: Rafał Kamiński (dyrektor)
Produkcja: Mariusz Gajda
Druk: Quad/Graphics Europe Sp. z o.o., Wyszków

Prenumerata i egzemplarze archiwalne:
tel. 22 3367901, infolinia 801000869;
e-mail: prenumerata.axel@qg.com (zamówienia)

Sprzedaż internetowa: www.literia.pl
Prenumerata zagraniczna: www.literia.pl
E-wydania: ksplus.pl

Redakcja nie zwraca materiałów niezamówionych, zastrzega sobie prawo redagowania nadesłanych tekstów, nie odpowiada za treść zamieszczanych reklam i ogłoszeń

Zabroniona jest bezumowna sprzedaż czasopisma po cenie niższej od ceny detalicznej ustalonej przez wydawcę. Sprzedaż numerów aktualnych i archiwalnych po innej cenie jest nielegalna i grozi odpowiedzialnością karną.

PRE ATA

KOMPUTER ŚWIATA

TYLKO 89 ZŁOTYCH

12 WYDAŃ KOMPUTER ŚWIATA

- Dogłębne testy sprzętu i programów
- Praktyczne porady
- Interesująca wiedza
- Gorące nowości
- Pełne wersje programów w każdym numerze
- E-wydanie zawsze gratis
- Atrakcyjne bonusy tylko dla Czytelników
- **Usługa KŚ+**: nowatorski i wygodny dostęp do programów z dowolnego komputera

ZAMÓW

PRENUMERATĘ JUŻ DZIŚ

INTERNET: kup na **www.ks.literia.pl**
E-MAIL: napisz na adres **prenumerata.axel@qg.com**
TELEFON: zadzwoń pod **22 349 90 71** lub **801 000 869**

OFERTY WAŻNE NA TERENIE POLSKI

ZAMÓW ROCZNĄ PRENUMERATĘ
MAGAZYNU FORBES

Więcej szczegółów na www.literia.pl/prenumerata-forbes